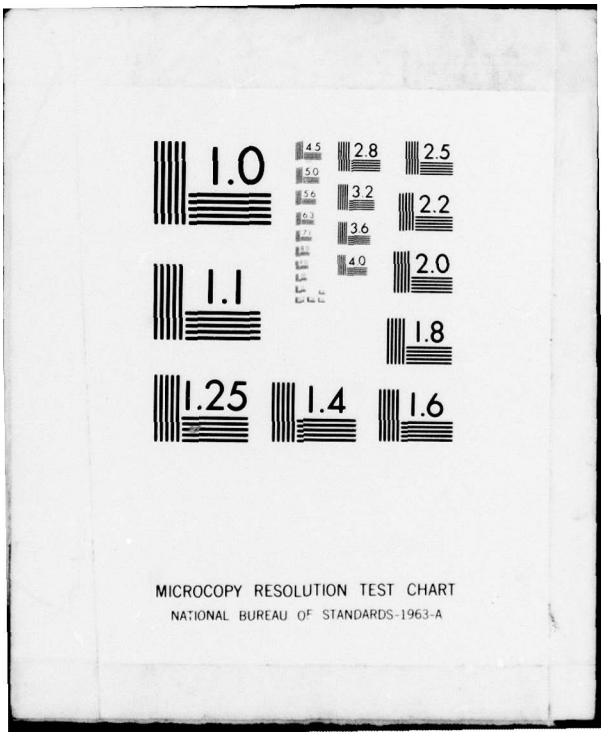
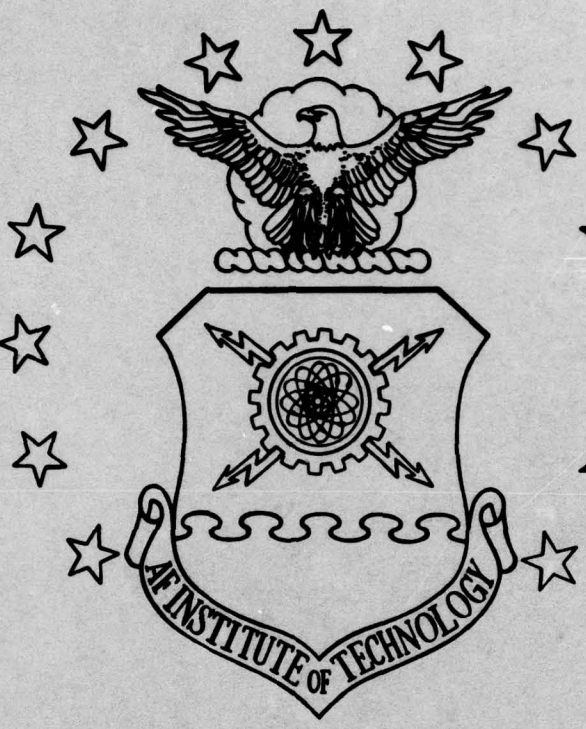
AD-A080 213 AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOO--ETC F/G 17/4
INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED--ETC(U)
DEC 79 T J HALL
UNCLASSIFIED AFIT/GE/EE/79-15 NL

1 OF 2
AD
A080213


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

LEVEL II



UNITED STATES AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GE/EE/79-15

INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED SPREAD SPECTRUM WAVEFORMS

THESIS

AFIT/GE/EE/79-15 Thomas J. Hall
Capt USAF

(14) AFIT/GE/EE/79-15

(6) # INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED SPREAD SPECTRUM WAVEFORMS.

(9) Master's THESIS

Presented to the Faculty of the School of Engineering
of the Air Force Institute of Technology
Air University
in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

(12) 118

by

(10) Thomas J. Hall B.S.
Capt USAF
Graduate Electrical Engineering

(11) 15 December 1979

Approved for public release; distribution unlimited

Preface

I would like to express my thanks to Maj J. Gobien of the Rome Air Development Center for suggesting the topic for my thesis. The generic modulation formats described within were also suggested by him.

I am grateful for the encouragement, guidance, and insight provided to me by my thesis advisor, Capt Stanley R. Robinson, over the duration of this effort. Special thanks also go to the readers, Maj J. Carl and Lt Col R. Carpinella of the Electrical Engineering Department at AFIT.

I wish to thank my wife, Kristy, for her patience, understanding, encouragement and support throughout and for the many hours of proof reading and typing. Finally, I want to thank my special helpers, Michael, Matthew, and Jeffrey, for the sacrifices they have made to let their father study.

Thomas J. Hall

Contents

List of Figures

List of Tables

Abstract

Direct sequence pseudo-noise encoded spread spectrum waveforms are examined for their vulnerability to unauthorized intercept and message decoding. The interceptor is assumed to be operating without the knowledge of the spreading code used. No attempt is made by the interceptor to duplicate the code in the analysis.

A general waveform equation is introduced to be used in the analysis. Two generic modulation formats, designated as format A and format B, and their associated transmitters are presented, and it is shown that format A and B both fit the general waveform equation.

An intercept receiver model is proposed that will decode transmissions that fit the form of the general waveform equation. The receiver is analyzed for its success in decoding both generic modulation formats. It is shown that for format A, decoding of the message without knowledge of the pseudo-noise code is not possible for this receiver when only one transmission is received. However, when two simultaneous transmissions are received, message decoding is possible. Factors that affect successful decoding in this case are the carrier phase differences between the two transmitters, the offset between the pseudo-noise code bits at the receiver, and additive noise. It is also shown that for modulation format B, decoding of the message is possible when only one transmission is received. Factors that affect

successful decoding in this case are additive noise, Doppler phase shift, and the extent to which the baseband modulation was linear.

INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED SPREAD SPECTRUM WAVEFORMS

I Introduction

Spread spectrum (SS) communications systems are those which are intentionally designed to transmit information over a bandwidth much wider than would normally be required. Since their beginnings in the early 1950's, SS systems have found both commercial and military applications. Some of the properties that have made the use of SS systems desirable are as follows (Ref. 6:6):

1) Selective addressing capability;
2) Code division multiplexing for multiple access;
3) Low density power spectra for signal hiding;
4) Message screening from eavesdroppers;
5) High resolution ranging;
6) Interference rejection.

The interference rejection property makes the use of SS communications systems attractive for use in a high density, multisignal environment where strong interfering signals would render a conventional narrowband system useless. An SS system, in theory, will demonstrate a robust immunity to strong interfering signals and jamming.

Problem Statement

The designer of an SS system intends that unauthorized eavesdropping be extremely difficult. A method used in the past for unauthorized demodulation has been for the interceptor to duplicate the spreading code used, and synchronously demodulate with this code. It has been shown in the literature (Ref. 16 and 17) that for a linearly generated periodic code of length 2^n-1 bits per period, the code can be reconstructed by observation of any 2n consecutive bits of the code. This method, however, can be made prohibitively impractical by using non-linear codes (Ref. 17). The purpose of this thesis is to show that for a class of modulation formats, intercept and demodulation of SS waveforms is possible without knowledge of the pseudo-noise spreading code, under appropriate conditions.

Scope

This thesis will consider only direct sequence generated SS systems. The level of presentation is directed toward the working communication engineer. Extensive mathematical derivations are an unavoidable necessity. Although an intercept receiver is proposed, no testing or experimentation will be accomplished. The intercept receivers operation is examined and performance predictions are made.

Assumptions

The following assumptions were made to narrow the problem to one that could be handled within the time allotted:

1. The interceptor is dedicated, knowledgeable, and properly equipped for SS signals. He knows the general frequency and modulation characteristics of the transmitter, but not the pseudo-noise keying codes used. He can adjust his hardware to fit a particular situation.

2. The interceptor is not interested in just detecting the presence of an SS signal, but rather he desires real-time message reconstruction.

3. Linearly generated codes are not used because of their ease of reconstruction by the interceptor.

4. The interceptor is limited by practical considerations to a "simple" receiver, that is, one that does not entail a great deal of sophistication such as the use of a massive computer center for message processing.

5. The interceptor is situated in a multisignal tactical war environment.

Approach and Sequence of Presentation

The approach used in this thesis is to examine the effect of processing direct sequence modulated SS waveforms through non-linear elements: square law and fouth law devices. Although there are many ways to attack the intercept and decoding problem, this particular approach was used because performing squaring and quadrupling operations on pseudo-noise code modulated waveforms generates terms that are independent of the code. The results of these non-linear operations are then examined for possible exploitation. The sequence of presentation is as follows. First, a

chapter is devoted to an introduction to the basic fundamentals of SS systems. Next, a general waveform equation is introduced that encompasses several different modulation formats. The general waveform equation takes pulse shaping of the data into account for offset quaternary phase shift keying, minimum shift keying, and sinusoidal frequency shift keying modulation schemes. Two generic spread spectrum modulation formats, designated as format A and B, and their associated transmitters are introduced for eventual analysis of their vulnerability to intercept. The generic modulation formats are shown to fit the general waveform equation.

In the next chapter, an intercept receiver model is proposed. The receiver is analyzed with the general waveform equation as its input. The receiver is divided into general sections designated as the Carrier Reconstruction Loop, the Format A Decoder, and the Format B Decoder. The sections are analyzed in that order. It is shown that regardless of the modulation format or pulse shaping used, a signal is developed in the output of the quadrupling circuit of the Carrier Reconstruction Loop that is free of pseudo-noise encoding. Coherent carrier references are derived from this signal, and it is shown that in the case of modulation format B, the signal contains the desired message information. Next, it is shown that for modulation format A, decoding the message without knowledge of the pseudo-noise code used is not possible for this receiver when only one transmission is received. However, when two simultaneous

transmissions are received, message decoding is possible under appropriate conditions. Successful decoding in this case is dependent upon the carrier phase differences between the two transmitters, the arrival offset between the pseudo-noise code bits at the receiver, and additive noise. These effects are included in the output equations. Reconstruction of the message from the output equations is demonstrated for ideal conditions (i.e., negligible noise, synchronized carriers, and no code bit offset). Finally, it is shown that for modulation format B, decoding of the message is possible even when only one transmission is received. Additive noise, Doppler phase shift, and the linearity of the baseband modulation affect the success of decoding this format.

II Fundamentals of Spread Spectrum Communications Systems

The term "spread spectrum" is applied to any of a number of signaling techniques in which the transmitted waveform occupies a bandwidth far in excess of the baseband signal (Ref. 9) and where the envelope of the power spectral density of the transmitted waveform is not related to the data. These techniques generally fall into four categories (Ref. 7:1):

1) Direct sequence modulated;

2) Frequency hopping;

3) Time hopping;

4) Pulse-FM or chirp.

Direct sequence signals are generated by modulating a carrier with some code sequence. In this type of system, the incoming information signal is generally transformed into some digital format and then, assuming binary data, it is added modulo two to a higher speed code sequence. The combined information and code are then used to suppressed-carrier modulate an RF carrier. The high speed code sequence dominates the modulating sequence and determines the transmission bandwidth which is "spread" in comparison to the information bandwidth.

In a frequency hopping system, the carrier frequency is moved around in frequency. The frequency used at any particular time is determined by a code sequence. This code

sequence is the same type that is used in direct sequence systems except that the code clock rate is generally much smaller because of technological considerations.

In a time hopping system, the transmission time and period are controlled with a code sequence. Time hopping can be viewed as pulse modulation under code sequence control. Often, time hopping is used in conjunction with frequency hopping.

Pulse-FM or chirp is a technique commonly used in radar systems. This technique does not use coding to spread the transmitted signal bandwidth as the others do, but uses swept-frequency pulses. The receiver employs a dispersive filter to match the swept signal and compress it into a much narrower time slot.

This thesis will be limited to consideration of direct sequence modulated SS systems because of their more common usage at the present level of technology.

Spread Spectrum Communications System Model

Figure 1 illustrates the basic components of a direct sequence modulated SS communications system using binary phase shift keyed (BPSK) signaling. The message waveform, $m(t)$, is a bipolar binary sequence with $m(t) = \pm 1$. (Note that multiplication of a carrier by plus one or minus one is equivalent to shifting the phase by zero or π radians respectively.) The phase modulated carrier is multiplied by the spreading waveform, $c(t)$, a high rate binary sequence commonly referred to as a pseudo-random (PR) or pseudo-noise (PN)

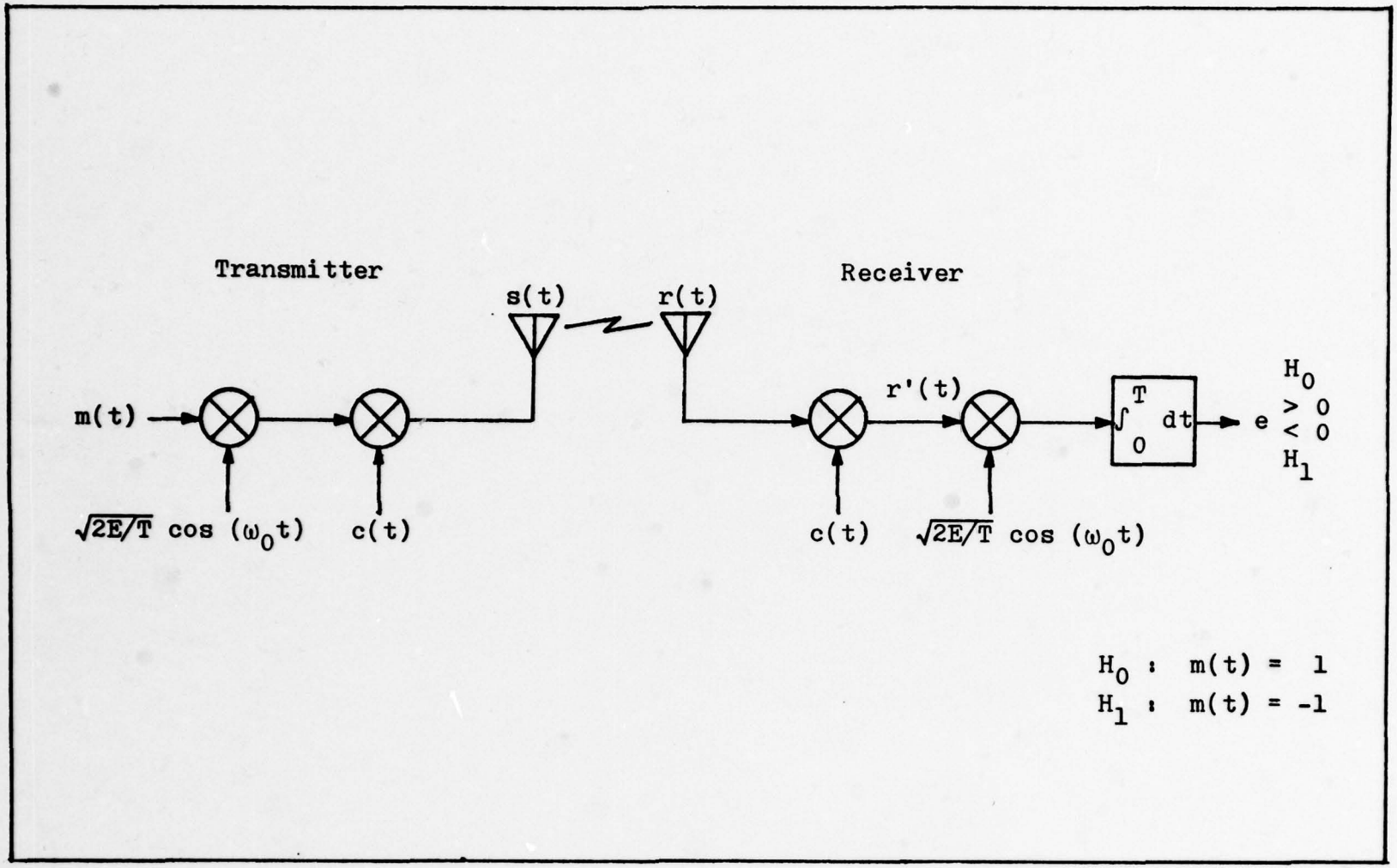


Figure 1. Spread Spectrum Communications System Model.

sequence.[1] These designations are a consequence of the fact that the sequence generates sample statistics similar to a random, noiselike waveform. However, the sequence c(t) is completely deterministic and periodic. For extremely high signaling rates, the spectrum of the sequence is so spread and the spectral density so low that to the casual observer it appears to be background noise. The spreading waveform, c(t), takes on values of ±1 in order to accomplish the required phase shifting.

The receiver has a replica of the spreading code which is multiplied by the received signal to strip the code off of the signal.[2] The signal is then processed thru a correlation detector whose output is the sufficient statistic, e. From the sufficient statistic, a decision is made as to which of two hypothesis is true. Under one hypothesis, H_0, $m(t) = 1$. Under the other hypothesis, H_1, $m(t) = -1$.

It is clear that the difference between this system and conventional ones is multiplication by the PN sequence, c(t), at the transmitter and receiver. To understand the effect of c(t) on the system, the characteristics of PN sequences must be understood.

---

[1]The rate of the spreading waveform, c(t), is typically on the order of megabits per second, while the rate of the message, m(t), is typically on the order of kilobits per second.

[2]Note that $c^2(t) = 1$.

Characteristics of PN Sequences

Consider a random binary sequence. Such a sequence could be generated by repeatedly flipping a "fair" coin and recording the results, "one" for a head, "minus one" for a tail. The resulting random sequence will have the following three "randomness properties" (Ref. 10:10 and 15:279):

1) The Balance Property. The number of ones will be approximately equal to the number of minus ones.

2) The Run Property. Among the runs of consecutive ones and of zeroes, about one-half of the runs of each kind are of length one, one-fourth of each kind of length two, one-eighth of length three, and so on.

3) The Correlation Property. The expected value of the autocorrelation function of the sequence would be maximum at the origin and decrease rapidly away from the origin. PN sequences exhibit all three of these randomness properties.

A PN sequence is made up of bits of duration T_c and, to be consistent with the model under consideration, will be considered to have an amplitude of ±1. It is assumed that the sequence is continuous, that is, there is no space between bits; that the positive and negative bits occur with equal probability; and that successive pulses are statistically independent. Figure 2.a illustrates a portion of a typical PN sequence, c(t).

The autocorrelation function, $R_c(\tau)$, of the deterministic PN sequence, c(t), is the time average, strictly over all time, of the sequence multiplied by a time shifted

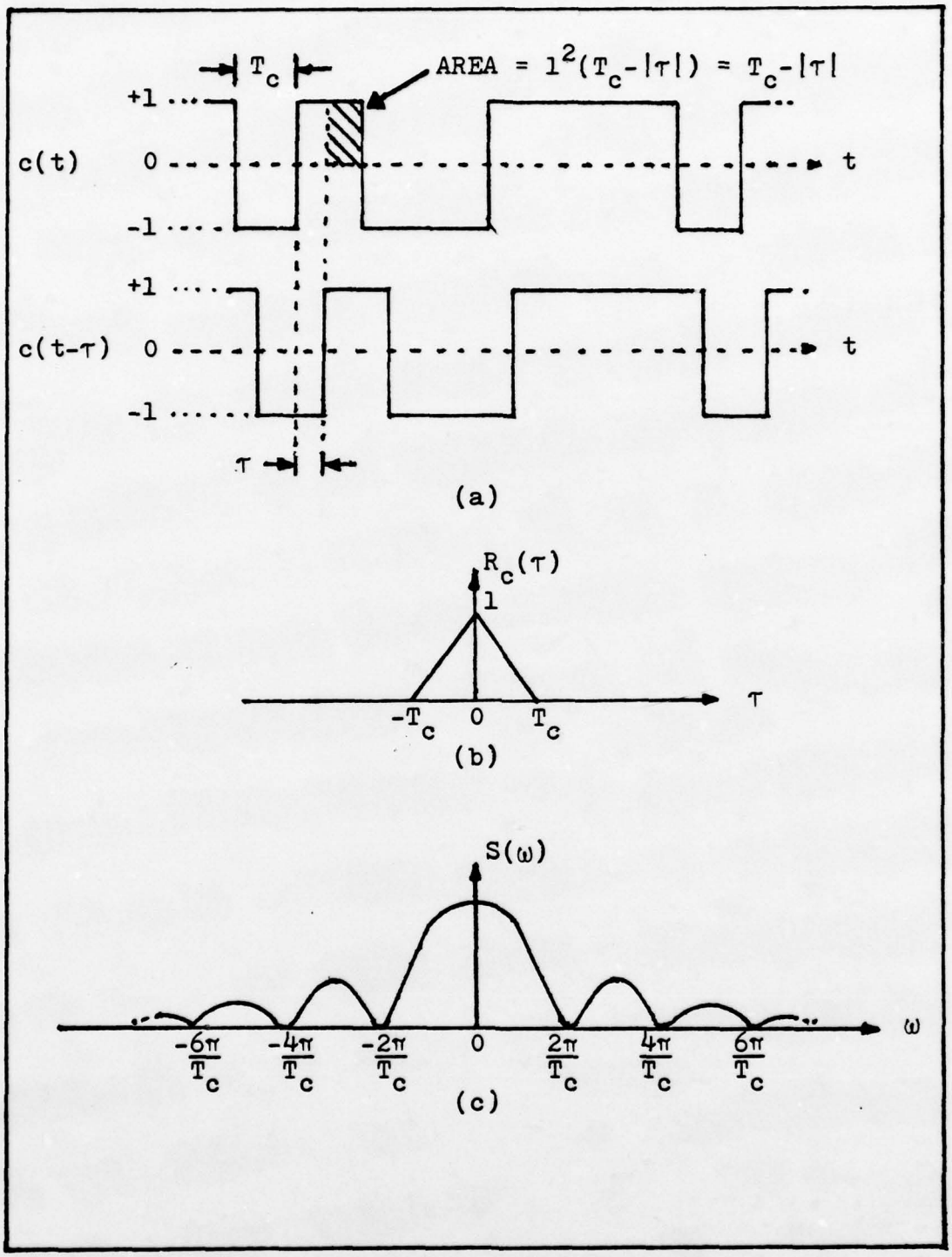


Figure 2. Autocorrelation Function and Power Spectral Density of a PN Sequence. (a) Typical Code Sequence. (b) Autocorrelation Function. (c) Power Spectral Density (Ref. 12).

version of itself (Ref. 12). Although a PN sequence is periodic, it is assumed that the period, T, is greater than the duration of the mission. Thus, for all practical purposes, the PN code period can be considered infinite. Then, the autocorrelation function is given by (Ref. 12)

$$R_c(\tau) = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} c(t)\, c(t+\tau)\, dt \qquad (1)$$

where τ represents the amount of the shift.

From the randomness properties of PN sequences, it is clear that for $|\tau|>T_c$, the average value of $c(t)\cdot c(t+\tau)$ is zero since its instantaneous value has an equal probability of being +1 or -1. For $|\tau|\leq T_c$, the average value over one bit of $c(t)\cdot c(t+\tau)$ is given by the area of the overlapping part of the displaced bits, shown shaded in Figure 2.a, divided by T_c. This area is given by $T_c-|\tau|$. Thus

$$R_c(\tau) = \begin{cases} \frac{1}{T_c}(T_c-|\tau|) & \text{for } |\tau| \leq T_c \\ 0 & \text{for } |\tau| > T_c \end{cases} \qquad (2)$$

$R_c(\tau)$ is plotted in Figure 2.b.

The power spectral density (PSD), $S_c(\omega)$, for a PN sequence is found from the autocorrelation function, $R_c(\tau)$, using the Wiener-Khintchine theorem:

$$S_c(\omega) = \int_{-\infty}^{\infty} R_c(\tau)\, e^{-j\omega\tau}\, d\tau \qquad (3)$$

Since $R_c(\tau)$ is an even function, this takes the form

$$S_c(\omega) = \int_{-\infty}^{\infty} R_c(\tau) \cos(\omega\tau)\, d\tau \qquad (4)$$

Then inserting $R_c(\tau)$ and exploiting symmetry gives

$$S_c(\omega) = \frac{2}{T_c} \int_0^{T_c} (T_c - |\tau|) \cos(\omega\tau)\, d\tau$$

$$= T_c \frac{\sin^2(\omega T_c/2)}{(\omega T_c/2)^2} \qquad (5)$$

$S_c(\omega)$ is shown in Figure 2.c.

Performance of Spread Spectrum System

Referring to Figure 1, the transmitted waveform of the SS model is given by

$$s(t) = \sqrt{2E/T}\, m(t)\, c(t) \cos(\omega_0 t) \qquad 0 \le t \le T \qquad (6)$$

where T, the message bit interval, is some integer multiple of T_c, the code bit interval ($T = NT_c$). The received signal is given by

$$r(t) = s(t) + n(t) \qquad (7)$$

where n(t) is zero mean, white, Gaussian noise with PSD of $S_n(\omega) = N_0/2$, and is independent of the code, c(t). The received waveform is multiplied by a stored replica of the code to give the following (assuming perfect synchronization):

$$r'(t) = \sqrt{2E/T}\, m(t)\, c^2(t) \cos(\omega_0 t) + c(t)\, n(t)$$

$$= \sqrt{2E/T}\, m(t) \cos(\omega_0 t) + n'(t) \tag{8}$$

The autocorrelation function of n'(t) is given by the following equation:

$$\begin{aligned} R'(t_1,t_2) &= E\{n'(t_1)\, n'(t_2)\} \\ &= E\{c(t_1)\, c(t_2)\}\, E\{n(t_1)\, n(t_2)\} \\ &= R_c(t_1-t_2)\, (N_0/2)\, \delta(t_1-t_2) \end{aligned} \tag{9}$$

Because of the delta function, this has value only when t_1 equals t_2. Then

$$\begin{aligned} R'(t_1-t_2) &= R_c(0)\, (N_0/2)\, \delta(t_1-t_2) \\ &= (N_0/2)\, \delta(t_1-t_2) \end{aligned} \tag{10}$$

Thus, n'(t) is itself white, Gaussian noise. The problem is thus reduced to determining whether H_0 or H_1 is true using binary antipodal signaling in white, Gaussian noise. The well known probability of error, P(E), for this case is

$$P(E) = \text{erfc}(\sqrt{2E/N_0}) \tag{11}$$

where the message bits are assumed equally likely and where the error function compliment (erfc) is defined as

$$\text{erfc}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-y^2/2)\, dy \tag{12}$$

Thus, in the case of interference by white, Gaussian noise, the performance of the SS system is identical to a conventional system.

The real advantage of the use of an SS system is in the presence of a strong narrowband interfering signal

centered about the carrier frequency. Let the interfering signal, $n_J(t)$, be zero mean and Gaussian with PSD $S_J(\omega)$ as shown in Figure 3. The received signal is now

$$r(t) = s(t) + n(t) + n_J(t) \tag{13}$$

and hence

$$\begin{aligned} r'(t) &= \sqrt{2E/T}\, m(t) \cos(\omega_0 t) + c(t)\,[n(t) + n_J(t)] \\ &= \sqrt{2E/T}\, m(t) \cos(\omega_0 t) + n''(t) \end{aligned} \tag{14}$$

The autocorrelation function of $n''(t)$ is given by

$$\begin{aligned} R''(t_1,t_2) &= E\{n''(t_1)\, n''(t_2)\} \\ &= E\{c(t_1)\, c(t_2)\} \\ &\quad \cdot E\{[n(t_1) + n_J(t_1)]\,[n(t_2) + n_J(t_2)]\} \\ &= R_c(t_1-t_2)\,[E\{n(t_1)\, n(t_2)\} + E\{n(t_1)\, n_J(t_2)\} \\ &\quad + E\{n_J(t_1)\, n(t_2)\} + E\{n_J(t_1)\, n_J(t_2)\}] \end{aligned} \tag{15}$$

Since $n(t)$ and $n_J(t)$ are independent of each other, the autocorrelation becomes

$$R''(t_1,t_2) = R_c(t_1-t_2)\,[(N_0/2)\,\delta(t_1-t_2) + R_J(t_1-t_2)] \tag{16}$$

With $\tau = t_1-t_2$, the autocorrelation of the interfering signal is found by taking the inverse Fourier transform of $S_J(\omega)$.

$$\begin{aligned} R_J(\tau) &= \frac{1}{2\pi} \int_{-\infty}^{\infty} S_J(\omega)\, e^{j\omega\tau}\, d\omega \\ &= \frac{1}{\pi} \int_{\omega_0-B/2}^{\omega_0+B/2} (J_0/2B)\, e^{j\omega\tau}\, d\omega \\ &= J_0\, \frac{\sin(\pi B\tau)}{\pi B\tau} \cos(\omega_0\tau) \end{aligned} \tag{17}$$

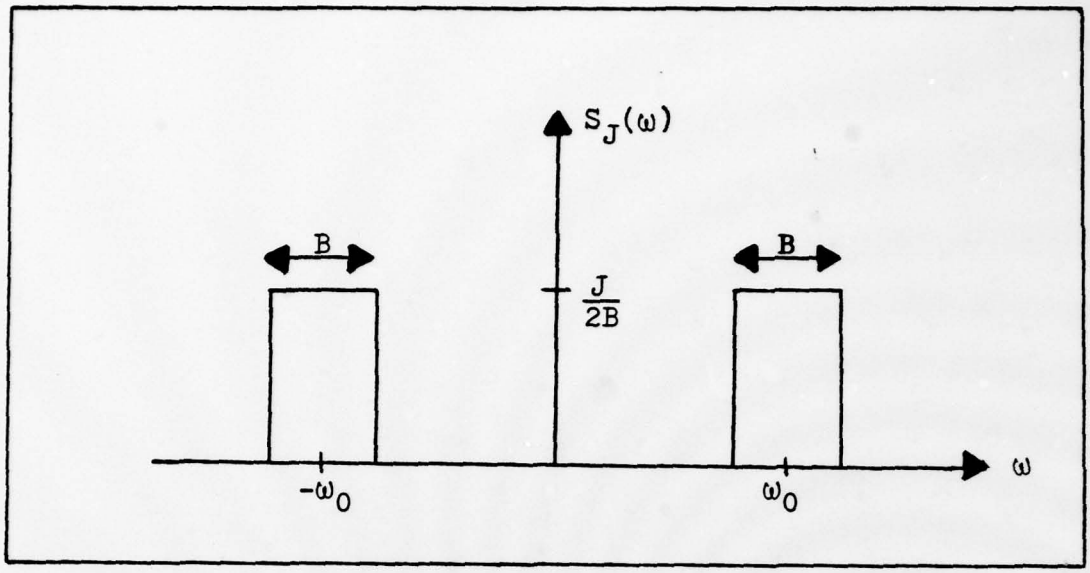


Figure 3. Power Spectral Density of Interfering Signal, $n_J(t)$.

The autocorrelation function of n"(t) then becomes the following:

$$R"(\tau) = R_c(\tau)\,(N_0/2)\,\delta(\tau) + R_c(\tau)\,\frac{J_0\,\sin(\pi B\tau)}{\pi B\tau}\,\cos(\omega_0\tau)$$

$$= (N_0/2)\,\delta(\tau) + R_c(\tau)\,\frac{J_0\,\sin(\pi B\tau)}{\pi B\tau}\,\cos(\omega_0\tau) \qquad (18)$$

Now let B→0. This corresponds to narrowband jamming. Then the PSD of R"(τ) is the following:

$$S"(\omega) = \int_{-\infty}^{\infty} (N_0/2)\,\delta(\tau)\,e^{-j\omega\tau}\,d\tau$$

$$+ \int_{-\infty}^{\infty} R_c(\tau)\,J_0\,\cos(\omega_0\tau)\,e^{-j\omega\tau}\,d\tau$$

$$= (N_0/2) + (1/2)\,J_0T_c\,\frac{\sin^2[(\omega-\omega_0)T_c/2]}{[(\omega-\omega_0)T_c/2]^2}$$

$$+ (1/2)\, J_0 T_c \frac{\sin^2[(\omega+\omega_0)T_c/2]}{[(\omega+\omega_0)T_c/2]^2} \qquad (19)$$

$S''(\omega)$ is shown in Figure 4. Since the data pulse duration, T, is typically several orders of magnitude greater than the code pulse duration, T_c, the bandwidth of $c(t)\cdot n_J(t)$ is much wider than the bandwidth of $c(t)\cdot s(t)$. Over the message bandwidth, the PSD of $c(t)\cdot n_J(t)$ is approximately flat and is viewed by the correlation detector as an additive "white" noise term. Using this approximation, equation (19) becomes

$$S''(\omega) \approx (N_0/2) + (J_0 T_c/2) \qquad (20)$$

The probability of error in deciding whether m(t) was a plus one or a minus one is thus

$$P(E) = \text{erfc}[\sqrt{2E/(N_0+J_0T_c)}] \qquad (21)$$

If the PN code was not used in the system, corresponding to $c(t) = 1$, then the autocorrelation of the noise is (with $B \to 0$)

$$R''(\tau) = (N_0/2)\,\delta(\tau) + J_0 \cos(\omega_0\tau) \qquad (22)$$

and the PSD of the noise is

$$S''(\omega) = (N_0/2) + (J_0/2)\,\delta(\omega+\omega_0) + (J_0/2)\,\delta(\omega-\omega_0) \qquad (23)$$

To determine the associated P(E) for this case, the mean and variance of the sufficient statistic, e, must be calculated. In this case

$$e = 2E/T \int_0^T m(t) \cos^2(\omega_0 t)\, dt$$

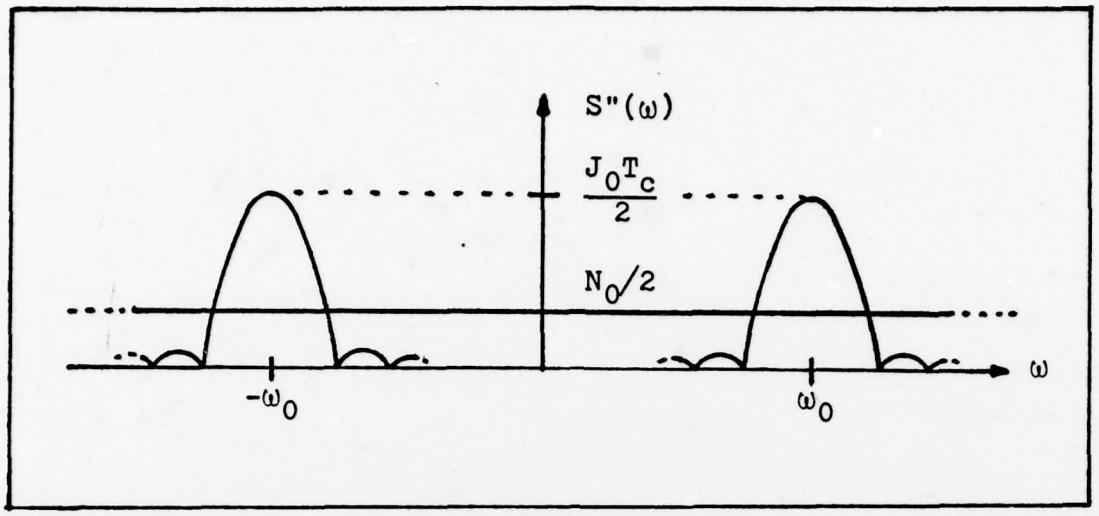


Figure 4. Power Spectral Density of n"(t).

$$+ \sqrt{2E/T} \int_0^T n(t) \cos(\omega_0 t)\, dt$$

$$+ \sqrt{2E/T} \int_0^T n_J(t) \cos(\omega_0 t)\, dt \qquad (24)$$

The conditional means are given by

$$E\{e|H_0\} = 2E/T \int_0^T E\{m(t)|H_0\} \cos^2(\omega_0 t)\, dt$$

$$+ \sqrt{2E/T} \int_0^T E\{n(t)|H_0\} \cos(\omega_0 t)\, dt$$

$$+ \sqrt{2E/T} \int_0^T E\{n_J(t)|H_0\} \cos(\omega_0 t)\, dt$$

$$= 2E/T \int_0^T \cos^2(\omega_0 t)\, dt = E = \bar{e}_0 \qquad (25)$$

and

$$E\{e|H_1\} = -E = \bar{e}_1 \qquad (26)$$

The conditional variance of the statistic, given either hypothesis, is identical and is given by the following (Ref. 20:177):

$$\begin{aligned} VAR(e|H_0) &= VAR(e|H_1) \\ &= 2E/T \int_0^T \int_0^T R''(t,u) \cos(\omega_0 t) \cos(\omega_0 u)\, dt\, du \\ &= (EN_0/2) + (EJ_0T/2) = \sigma^2 \end{aligned} \tag{27}$$

Thus, the probability density function (PDF) of the sufficient statistic, e, given either H_0 or H_1 is true, is Gaussian with mean $\bar{e}_0$ or $\bar{e}_1$, and variance σ^2. The associated probability of error in estimating the message sent is then

$$\begin{aligned} P(E) &= P(e>0|H_1)\, P(H_1) + P(e<0|H_0)\, P(H_0) \\ &= P(e<0|H_0) \\ &= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{0} \exp\left[-\frac{1}{2} \frac{(x-\bar{e}_0)^2}{\sigma^2}\right] dx = \operatorname{erfc}\left[\sqrt{\frac{2E}{N_0+J_0T}}\right] \end{aligned} \tag{28}$$

Equations (21) and (28) can now be compared to see the effect of the code, c(t). If N_0 is considered negligible, then the effect of the narrowband interference on the system performance was reduced from J_0T to J_0T_c. The improvement ratio is

$$\frac{J_0T}{J_0T_c} = \frac{T}{T_c} = N \tag{29}$$

This improvement thru the use of the PN code is commonly referred to as the processing gain of the SS system. Notice that it is roughly equivalent to the ratio of the SS trans-

mission bandwidth to the message bandwidth. Thus, it is desirable to use an SS system in an environment where strong narrowband interference is encountered. It should be noted that this analysis assumes that the jamming signal is uncorrelated with the code, c(t). For a repeater jammer, the result of this analysis would not be correct because of the correlation between the code and jamming signal.

The fundamental aspects of SS communications systems that have been presented in this chapter should equip the reader sufficiently for the development that follows. In the next chapter, a general waveform equation will be presented. This equation will be used as the primary tool in the analysis of the proposed intercept receiver model of chapter IV. In addition, two generic SS modulation formats will be introduced and shown to be equivalent to the general waveform equation.

mission bandwidth to the message bandwidth. Thus, it is desirable to use an SS system in an environment where strong narrowband interference is encountered. It should be noted that this analysis assumes that the jamming signal is uncorrelated with the code, c(t). For a repeater jammer, the result of this analysis would not be correct because of the correlation between the code and jamming signal.

The fundamental aspects of SS communications systems that have been presented in this chapter should equip the reader sufficiently for the development that follows. In the next chapter, a general waveform equation will be presented. This equation will be used as the primary tool in the analysis of the proposed intercept receiver model of chapter IV. In addition, two generic SS modulation formats will be introduced and shown to be equivalent to the general waveform equation.

III Generic Modulation Formats

In this section, a waveform equation will be introduced in a general form that encompasses many different modulation formats that are already well described in the literature. Two generic SS modulation formats, format A and B, and their associated transmitters will be introduced that will be analyzed in a later section for their vulnerability to intercept. Finally, it will be shown that the two generic modulation formats fit the general waveform equation.

General Waveform Equation

The SS modulation formats will be modeled in quadrature component form as (Ref. 2):

$$s(t) = I(t)\cos[\omega_0 t + \theta(t)] + Q(t)\sin[\omega_0 t + \theta(t)] \tag{30}$$

where

$$I(t) = \sum_n a_n p(t-nT_c) \tag{31}$$

$$Q(t) = \sum_n b_n p(t-nT_c-T_c/2) \tag{32}$$

and

$p(t)$ = pulse shaping function,

a_n = code and/or data dependent term, constant on the interval $nT_c - T_c/2 < t < nT_c + T_c/2$,

b_n = code and/or data dependent term, constant on the interval $nT_c < t < (n+1)T_c$,

T_c = code pulse duration,

and

$\theta(t)$ = phase term caused by data modulation (format B only).

The pulse shaping function, p(t), is determined by the specific RF modulation technique used. Three methods of RF modulation will be considered in this thesis: offset quaternary phase shift keying (O-QPSK); minimum shift keying (MSK); and sinusoidal frequency shift keying (SFSK). These methods are considered for the following reasons (Ref. 5):

1) These techniques exhibit minimal power spectral occupancy, which is desirable to an SS system designer who wants to minimize detectability of the signals.

2) Modern system non-linearities and power efficiencies constrain the modulation format to a constant envelope type, which these are. This has the added benefit of denying a potential interceptor any amplitude modulation information.

For these reasons, the SS system designer would very likely use one of the three techniques: O-QPSK, MSK, or SFSK.

For O-QPSK modulation, the pulse shaping function is given by

$$p(t) = \begin{cases} 1 & -T_c/2 < t < T_c/2 \\ 0 & \text{elsewhere} \end{cases} \qquad (33)$$

For MSK, the pulse shaping function is given by

$$p(t) = \begin{cases} \cos \frac{\pi t}{T_c} & -T_c/2 < t < T_c/2 \\ 0 & \text{elsewhere} \end{cases} \qquad (34)$$

For SFSK, the pulse shaping function is (Ref. 1)

$$p(t) = \begin{cases} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4} \sin\left(\frac{4\pi t}{T_c}\right)\right] & -T_c/2 < t < T_c/2 \\ 0 & \text{elsewhere} \end{cases} \qquad (35)$$

The three pulse shapes are shown in Figure 5. These three forms of modulation are identical except for the pulse shaping function (Refs. 1,2,5,11, and 18).

To get a clear picture of the general waveform described by equations (30) thru (32), and to understand the relationships between the terms, consider $\sum_n p(t-nT_c)$ and $\sum_n p(t-nT_c-T_c/2)$ for O-QPSK pulse shaping. These sums are shown in Figure 6. The second pulse stream is offset from the first by $T_c/2$ (half a code bit). If the following values of a_n and b_n are assumed, then I(t) and Q(t) are as shown in Figure 6:

$$a_{-2} = 1 \quad a_{-1} = -1 \quad a_0 = -1 \quad a_1 = 1 \quad a_2 = -1$$
$$b_{-2} = 1 \quad b_{-1} = 1 \quad b_0 = -1 \quad b_1 = -1 \quad b_2 = 1$$

Notice that over the interval $0 < t < T_c$, there are two terms of I(t) involved and one term of Q(t). Thus, to describe the waveform over any interval T_c seconds long requires two equations. The representation for the n^{th} interval, $[nT_c < t < (n+1)T_c]$, is the following:

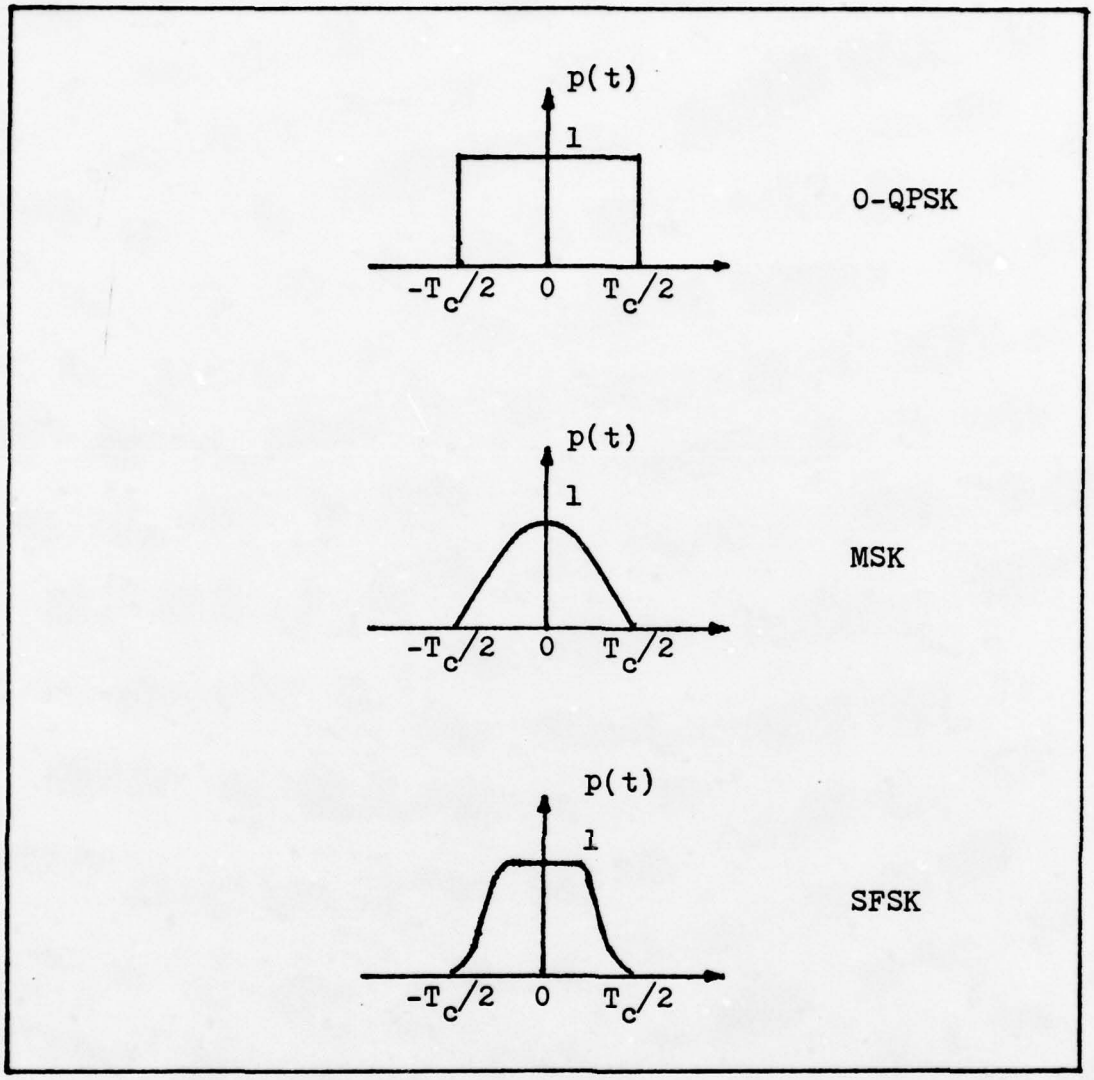


Figure 5. Pulse Shapes for O-QPSK, MSK, and SFSK Modulation

$$
\begin{aligned}
s(t) &= a_n p(t-nT_c)\cos[\omega_0 t + \theta(t)] \\
&\quad + b_n p(t-nT_c-T_c/2)\sin[\omega_0 t + \theta(t)] \\
&\qquad \text{for } nT_c < t < nT_c + T_c/2 \\
&= a_{n+1} p[t-(n+1)T_c]\cos[\omega_0 t + \theta(t)] \\
&\quad + b_n p[t-nT_c-T_c/2]\sin[\omega_0 t + \theta(t)] \\
&\qquad \text{for } nT_c + T_c/2 < t < (n+1)T_c
\end{aligned} \tag{36}
$$

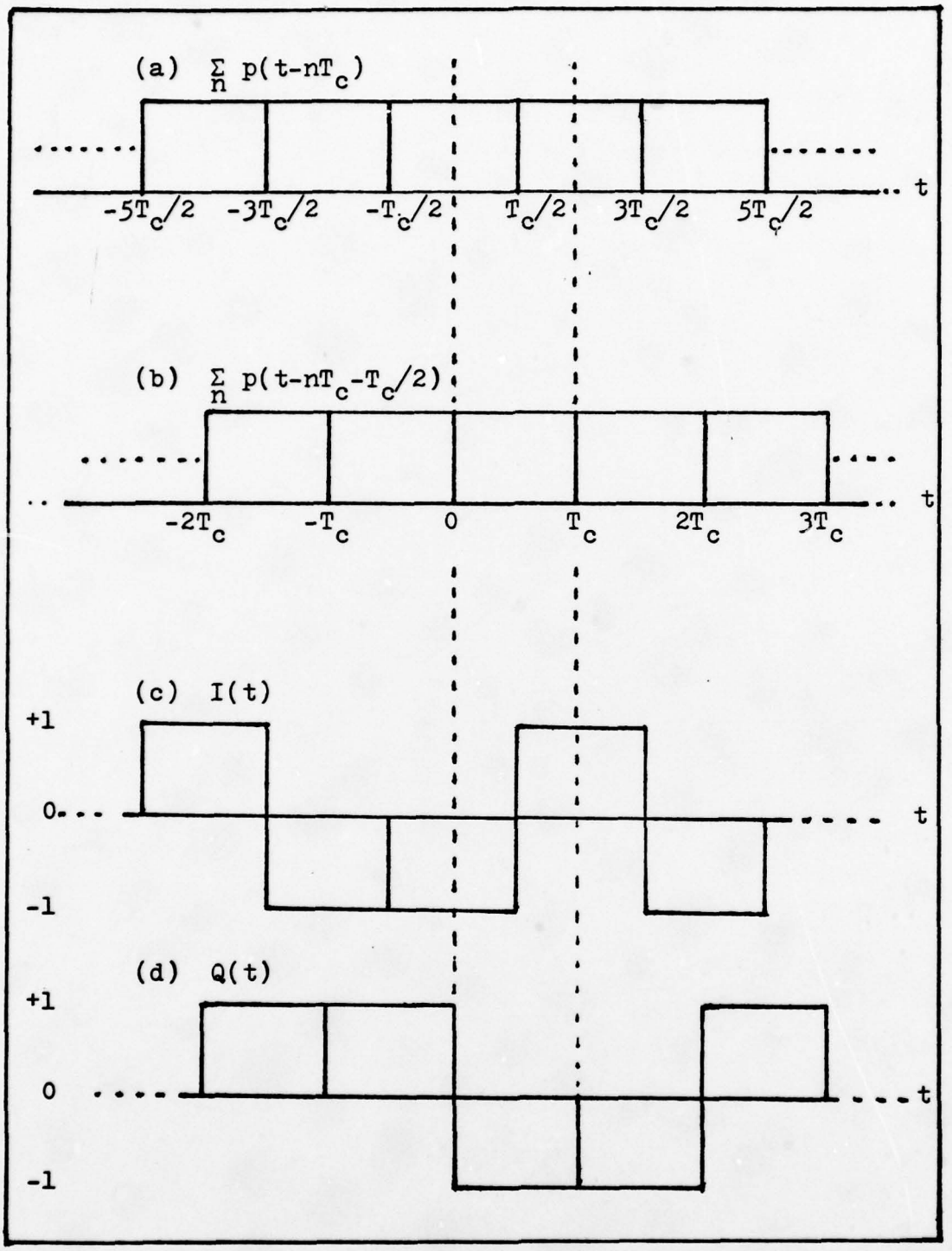


Figure 6. Relationship between I(t) and Q(t). (a) Pulse stream $\sum_n p(t-nT_c)$. (b) Pulse stream $\sum_n p(t-nT_c-T_c/2)$. (c) I(t). (d) Q(t).

This representation is general enough to accomodate a wide variety of digitized voice modulation techniques and will be used throughout this thesis, adapted to fit both generic modulation formats considered. Note that the only difference in the two parts of equation (36) is that in the second expression, the term a_{n+1} has replaced a_n, and $p[t-(n+1)T_c]$ has replaced $p(t-nT_c)$. Because this difference involves only a substitution of terms, only the first equation will be used in the intercept receiver calculations in chapter IV.

The two generic modulation formats and their transmitter models will next be described. The primary difference in the two models is that one scheme codes the data prior to modulation on carriers in quadrature (format A), while the other scheme directly modulates a carrier which is then coded at RF on quadratures (format B).

Generic Modulation Format A

Figure 7 illustrates the block diagram for the transmitter of this model. Pulse width modulation (PWM) is used to develop a "digitized" baseband signal. The baseband signal is split into an in-phase and quadrature channel where each is coded by one of two orthogonal[3] PN sequences, $c_I(t)$ and $c_Q(t)$.

In this model, a normalized speech-voltage waveform, $m(t)$, is sampled every T seconds to produce a stream of voice samples, $m_k = m(kT)$. The k^{th} sample is pulse width modulated

[3]Two codes are orthogonal if the expected value of their product is zero, i.e., $E\{c_I(t)c_Q(t)\} = 0$.

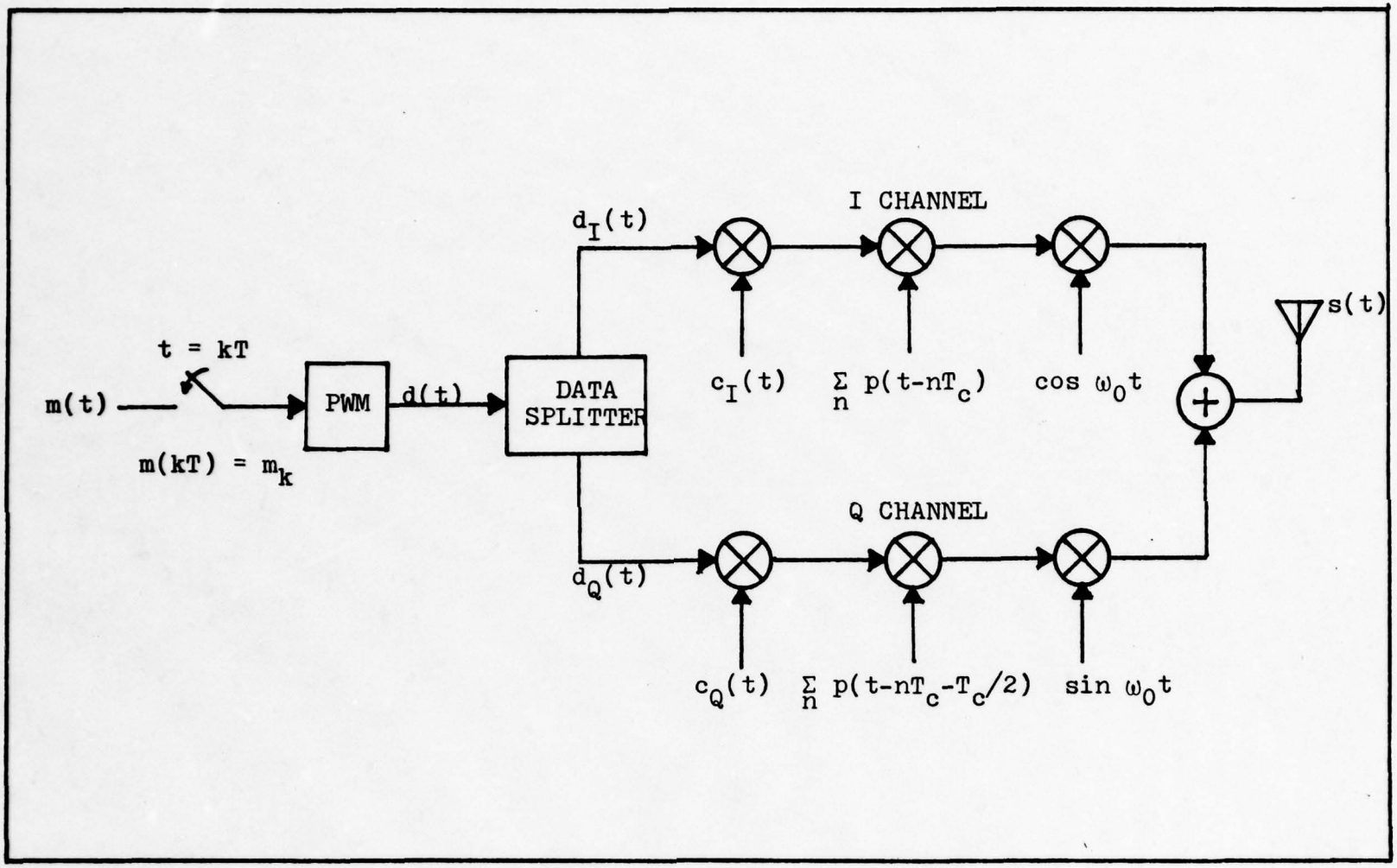


Figure 7. Generic Transmitter Model A.

to generate a pulse of variable width on the interval $kT < t < (k+1)T$, as is illustrated in Figure 8. Typical examples are shown for positive, negative, and zero level samples. The pulse width, τ_k, for the k^{th} voice sample is (Ref. 4)

$$\tau_k = (1+m_k)T/2 \tag{37}$$

Each T second sample interval of the pulse width modulated data stream, d(t), is divided into two T/2 sections. The first section is routed to the in-phase channel and the second to the quadrature channel. Each section, denoted $d_I(t)$ and $d_Q(t)$, contains a pulse whose width is doubled and the DC level is shifted to zero as shown in Figure 8. The data streams $d_I(t)$ and $d_Q(t)$ are bipolar with value

$$d_I(t) = \pm 1 \qquad d_Q(t) = \pm 1 \qquad d_I^2(t) = d_Q^2(t) = 1 \tag{38}$$

Note that there is a natural T/2 second offset in the start of each T second interval of $d_I(t)$ and $d_Q(t)$. For mathematical convenience, this offset will be ignored realizing that it must be accounted for in a real receiver. Thus, it will be assumed that each interval of $d_I(t)$ and $d_Q(t)$ is coincident prior to multiplication by a PN code.

The I and Q channel data are modulated by two orthogonal PN codes, $c_I(t)$ and $c_Q(t)$, with value

$$c_I(t) = \pm 1 \qquad c_Q(t) = \pm 1 \qquad c_I^2(t) = c_Q^2(t) = 1 \tag{39}$$

The transitions in the data streams, $d_I(t)$ and $d_Q(t)$, are

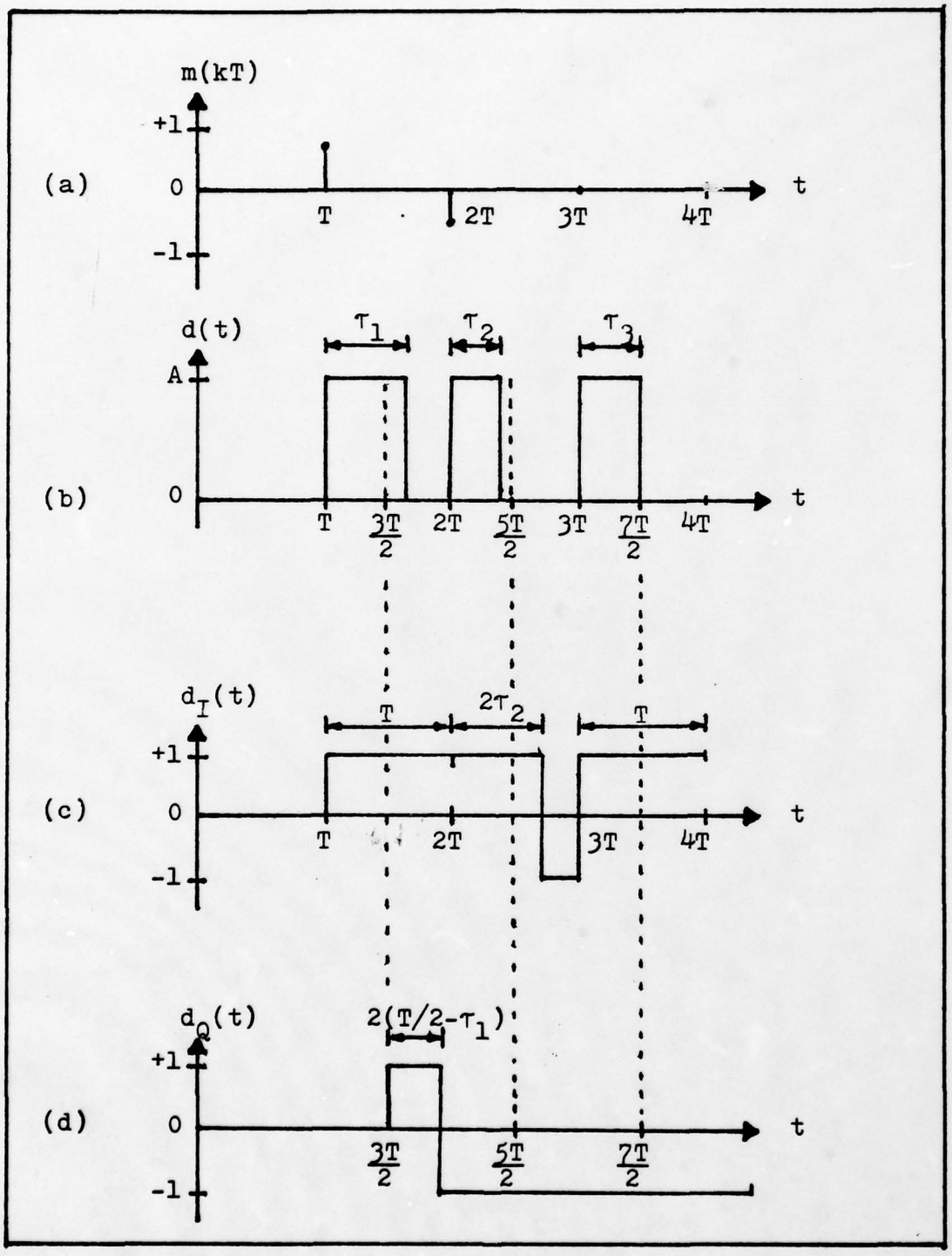


Figure 8. Transmitter Waveforms. (a) Sampled voice, m(kT). (b) Pulse width modulated samples, d(t). (c) In-phase channel data. (d) Quadrature channel data.

quantized such that they are synchronized with the code transitions so that the data is completely hidden by the code.

The modulated data streams are next multiplied by pulse shaping functions, $\sum_n p(t-nT_c)$ and $\sum_n p(t-nT_c-T_c/2)$, where $p(t)$ is as defined by one of equations (33) thru (35). The resultant products modulate in-phase and quadrature carriers, and are added to form the transmitted signal

$$s(t) = \sum_n c_{In}d_{In}p(t-nT_c)\cos(\omega_0 t) + \sum_n c_{Qn}d_{Qn}p(t-nT_c-T_c/2)\sin(\omega_0 t) \qquad (40)$$

where

c_{In} = n^{th} term of $c_I(t)$, constant on the interval $nT_c-T_c/2 < t < nT_c + T_c/2$,

c_{Qn} = n^{th} term of $c_Q(t)$, constant on the interval $nT_c < t < (n+1)T_c$,

d_{In} = value of $d_I(t)$, constant on the interval $nT_c - T_c/2 < t < nT_c + T_c/2$,

d_{Qn} = value of $d_Q(t)$, constant on the interval $nT_c < t < (n+1)T_c$.

For the n^{th} interval, $nT_c < t < (n+1)T_c$, the output signal is

$$\begin{aligned} s(t) &= c_{In}d_{In}p(t-nT_c)\cos(\omega_0 t) + c_{Qn}d_{Qn}p(t-nT_c-T_c/2)\sin(\omega_0 t) \\ &\qquad \text{for } nT_c < t < nT_c + T_c/2 \\ &= c_{I(n+1)}d_{I(n+1)}p[t-(n+1)T_c]\cos(\omega_0 t) + c_{Qn}d_{Qn}p(t-nT_c-T_c/2)\sin(\omega_0 t) \\ &\qquad \text{for } nT_c + T_c/2 < t < (n+1)T_c \end{aligned} \qquad (41)$$

Thus, it is seen that the output of transmitter model A is identical to the general equation, equation (36), with $a_n = c_{In}d_{In}$, $b_n = c_{Qn}d_{Qn}$, and $a_{n+1} = c_{I(n+1)}d_{I(n+1)}$.

Generic Modulation Format B

In the transmitter model for this modulation format, shown in Figure 9, a speech voltage waveform, m(t), is sampled every T seconds. The k^{th} sample, $m(kT) = m_k$, is mapped to a phase value, θ_k, by a non-linear differential amplitude to phase rule. The relationship between the voice sample and its corresponding phase value is

$$\theta_k = f(m_k) + \theta_{k-1} \tag{42}$$

where $f(m_k)$ is the non-linear mapping rule and θ_{k-1} is the phase value for the previous sample, m_{k-1}. The mapping rule is

$$f(m_k) = 2\,\mathrm{Cos}^{-1}\left(\frac{1+m_k}{2}\right) \tag{43}$$

Thus, m_k is found from successive phase values by

$$m_k = 2\cos\left(\frac{\theta_k-\theta_{k-1}}{2}\right) - 1 \tag{44}$$

The phase values directly modulate a carrier, $\cos(\omega_0 t)$, to produce, over all time, $\cos[\omega_0 t + \theta(t)]$. A quadrature carrier, $\sin[\omega_0 t + \theta(t)]$, is derived from this by passing thru a 90° phase shifter. These carriers are modulated by orthogonal PN codes; $c_I(t)$ and $c_Q(t)$, and pulse shaping data streams, $\sum_n p(t-nT_c)$ and $\sum_n p(t-nT_c-T_c/2)$, where these terms are as described previously. The in-phase and quadrature waveforms

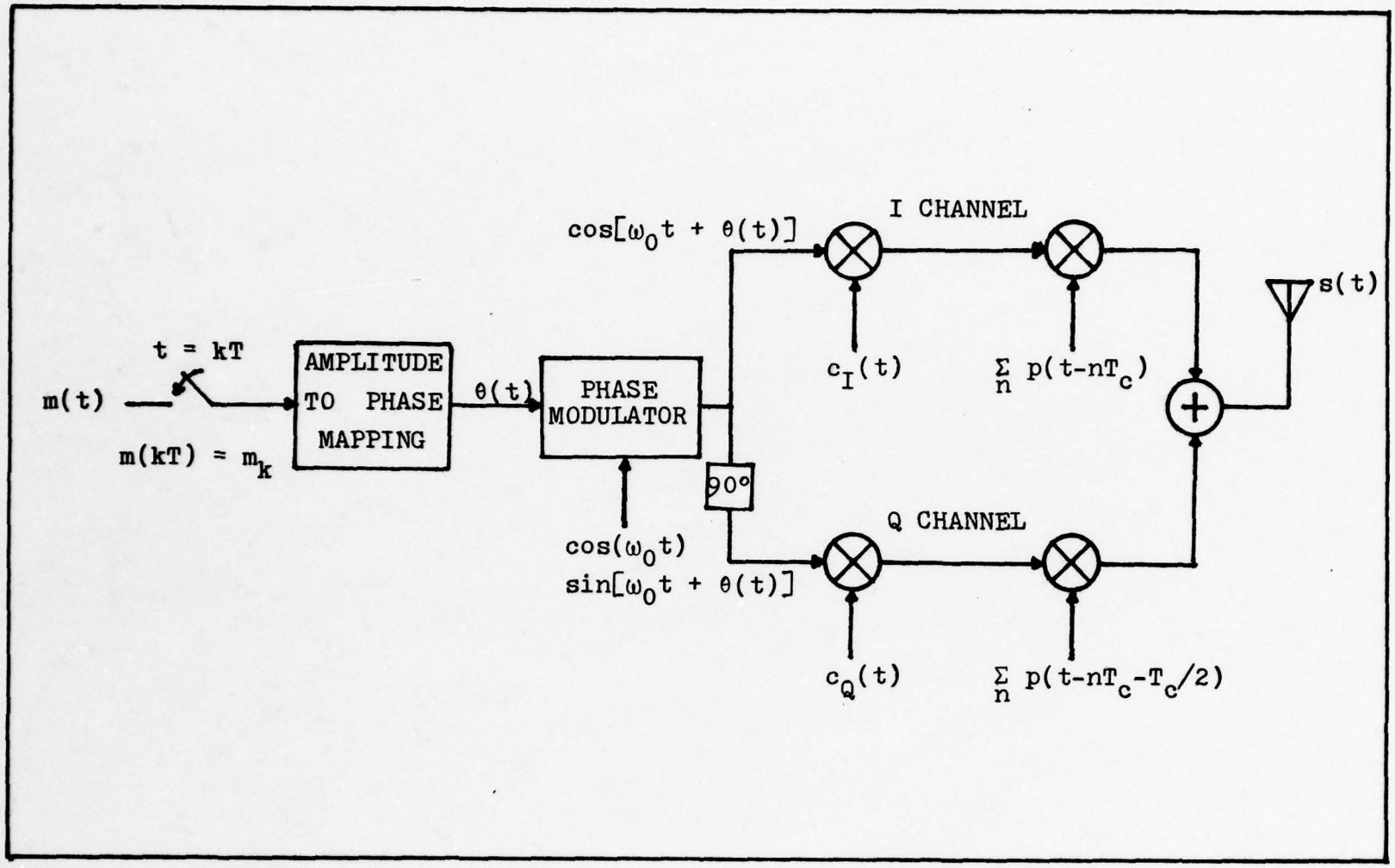


Figure 9. Generic Transmitter Model B.

are added to give the transmitted waveform

$$s(t) = \sum_n c_{In} p(t-nT_c) \cos[\omega_0 t + \theta(t)] + \sum_n c_{Qn} p(t-nT_c-T_c/2) \sin[\omega_0 t + \theta(t)] \qquad (45)$$

For the n^{th} interval, $nT_c < t < (n+1)T_c$, the transmitted signal is

$$\begin{aligned} s(t) &= c_{In} p(t-nT_c) \cos[\omega_0 t + \theta_n] \\ &\quad + c_{Qn} p(t-nT_c-T_c/2) \sin[\omega_0 t + \theta_n] \\ &\qquad \text{for } nT_c < t < nT_c + T_c/2 \\ &= c_{I(n+1)} p[t-(n+1)T_c] \cos[\omega_0 t + \theta_n] \\ &\quad + c_{Qn} p[t-nT_c-T_c/2] \sin[\omega_0 t + \theta_n] \\ &\qquad \text{for } nT_c + T_c/2 < t < (n+1)T_c \end{aligned} \qquad (46)$$

This is identical to the general equation (36) with $c_{In} = a_n$ and $c_{Qn} = b_n$.

It has been shown that both generic formats, A and B, fit the general waveform model given by equation (36). A proposed intercept receiver will be introduced in the next section, and the general waveform equation will be used to determine its outputs. The results will be applied to generic formats A and B.

IV Intercept Receiver Model and Analysis

In this chapter, a proposed intercept receiver model will be introduced. Using the general waveform equation developed in Chapter III as the transmitted waveform, the receiver outputs will be calculated and examined for exploitation and potential information recovery. It will be shown that under appropriate conditions, this receiver can successfully decode the transmitted message for both generic waveform models previously introduced.

Intercept Receiver Model

The proposed intercept receiver model is shown in Figure 10. The primary components are the sections labeled the Carrier Reconstruction Loop, the Format A Decoder, and the Format B Decoder. Each section will be treated in detail in the receiver analysis in the next subsection.

Some motivation for this particular structure is in order. This configuration represents the block diagram implementation of mathematical massaging of the general waveform equation to isolate modulation terms from PN code terms without the aid of PN code correlation. Recall from the discussion of the properties of PN codes that multiplying the code times a coherent replica eliminates the code, that is, $c^2(t) = 1$. The identical effect is produced by processing thru a non-linear element. The quadrupler in the Carrier Reconstruction Loop and the square law elements in

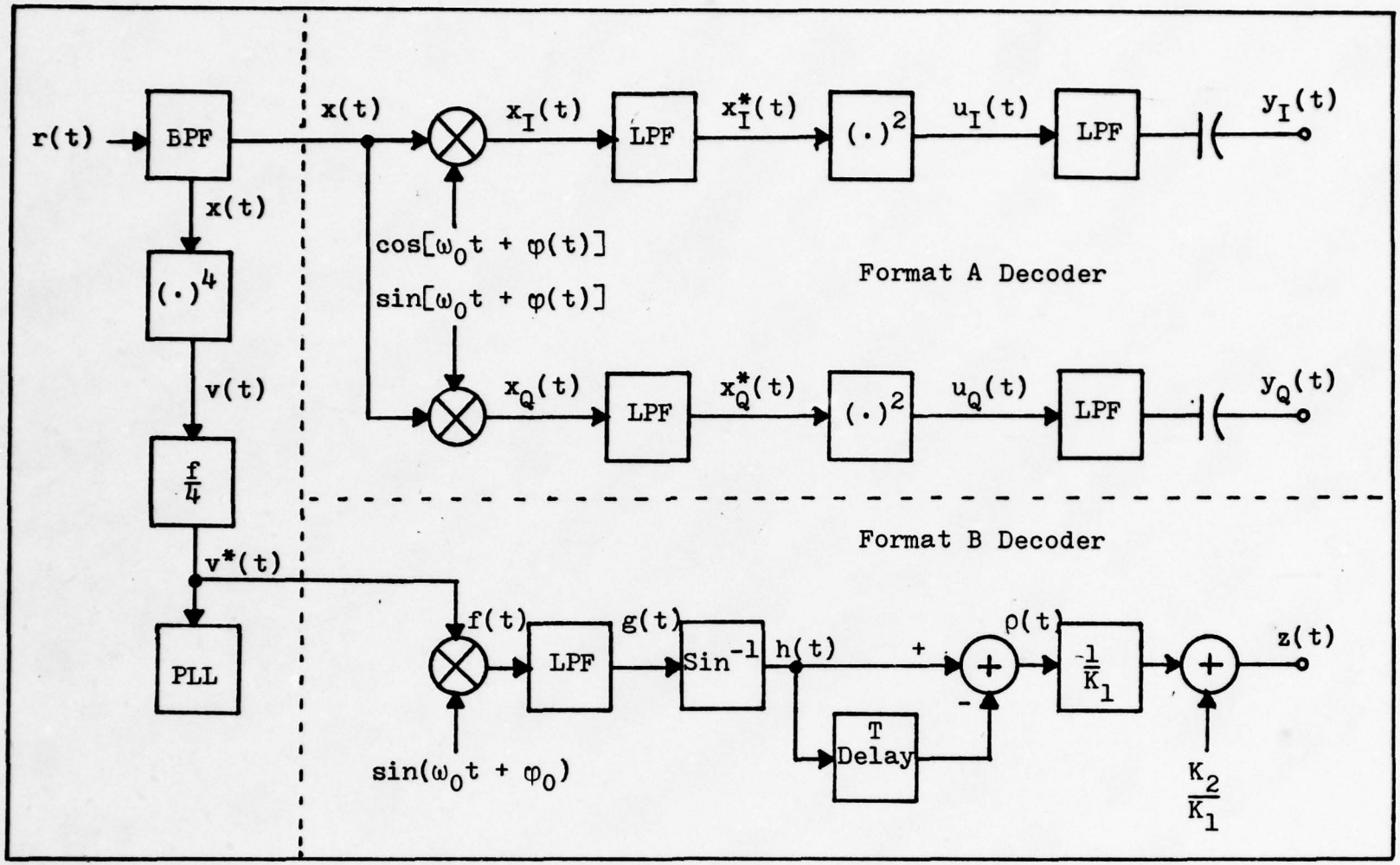


Figure 10. Intercept Receiver Model.

the Format A Decoder accomplish this purpose. The remaining hardware serves only to isolate the uncoded modulation terms and reduce interference and noise. The purpose of each element will become obvious as the receiver is analyzed.

Receiver Analysis

The received waveform is given by

$$r(t) = A(t) \sum_n a_n p(t-nT_c) \cos[\omega_0 t + \varphi(t)] + A(t) \sum_n b_n p(t-nT_c-T_c/2) \sin[\omega_0 t + \varphi(t)] + n(t) \quad (47)$$

where $A(t)$ is the amplitude of the received signal; $\varphi(t)$ is an instantaneous phase term that includes arrival phase offsets, Doppler phase shifts, and may include modulation (format B); $n(t)$ is modeled as zero-mean, white, Gaussian noise with two sided PSD height $N_0/2$; and a_n, b_n, $p(t-nT_c)$, and $(t-nT_c-T_c/2)$ are as defined in equations (31) and (32). Over one bit interval of the PN code, $nT_c < t < (n+1)T_c$, the received signal is

$$r(t) = Aa_n p(t-nT_c) \cos[\omega_0 t + \varphi(t)] + Ab_n p(t-nT_c-T_c/2) \sin[\omega_0 t + \varphi(t)] + n(t) \quad \text{for } nT_c < t < nT_c + T_c/2 \quad (48)$$

and

$$r(t) = Aa_{n+1} p[t-(n+1)T_c] \cos[\omega_0 t + \varphi(t)] + Ab_n p(t-nT_c-T_c/2) \sin[\omega_0 t + \varphi(t)] + n(t) \quad \text{for } nT_c + T_c/2 < t < (n+1)T_c \quad (49)$$

In equations (48) and (49), it has been assumed that the

signal amplitude remains constant over the code bit interval. Notice that the only difference in the two equations is that in the second, a_{n+1} replaces a_n and $p[t-(n+1)T_c]$ replaces $p(t-nT_c)$. Because this difference involves only a substitution of terms, equation (48) will be used as the basis for the succeeding development.

The received signal is filtered by a bandpass filter (BPF) with bandwidth (BW) B proportional to the reciprocal of the code pulse duration ($B \approx 2/T_c$). Thus, the assumption is being made that the transmission bandwidth B includes only the main lobe[4] of the spectrum of the transmitted signal. The filter is centered at the carrier frequency, f_0. The signal out of the filter is the following:

$$x(t) = [Aa_n p(t-nT_c) + n_c(t)] \cos[\omega_0 t + \varphi(t)] + [Ab_n p(t-nT_c-T_c/2) - n_s(t)] \sin[\omega_0 t + \varphi(t)] \quad (50)$$

In this equation, $n_c(t)$ and $n_s(t)$ are the in-phase and quadrature components of the bandlimited noise at the output of the filter (Ref. 22:237). The noise components are Gaussian with

$$E\{n_c(t)\} = E\{n_s(t)\} = E\{n(t)\} = 0 \quad (51)$$

$$E\{n_c^2(t)\} = E\{n_s^2(t)\} = E\{n^2(t)\} = (N_0)\cdot(\text{Noise BW}) \quad (52)$$

where the noise bandwidth equals the bandwidth of the filter preceeding it.

---

[4]Refer to Figure 2.c of Chapter II for a typical baseband spectrum after coding. The "main lobe" refers to the portion of the spectrum between $-2\pi/T_c$ and $2\pi/T_c$.

At this point the filtered signal, x(t), is processed thru the Carrier Reconstruction Loop and the Format A Decoder. The Carrier Reconstruction Loop will be considered first, followed by the Format A Decoder. The Format B Decoder will be considered last.

Carrier Reconstruction Loop. The Carrier Reconstruction Loop, Figure 11, serves two purposes in the intercept receiver. As its name implies, one purpose is to establish a coherent carrier reference in the receiver. The configuration shown is a special case of the N^{th} power loop described by Lindsey and Simon (Ref. 13:71-74). They show that a coherent carrier is produced at the output of the phase lock loop (PLL) for rectangular shaped data. Since the operation of the PLL is well documented in the literature (Ref. 8,13, 19 and 21), no treatment will be given here. It will be shown in Appendix A, however, that for MSK and SFSK pulse shaping, a signal similar to the rectangular pulse shape case is available to the PLL for tracking. Thus, the Carrier Reconstruction Loop will generate a coherent carrier in all cases of interest here.

The second purpose that the Carrier Reconstruction Loop serves is to provide a signal to the Format B Decoder that contains the desired modulation terms but no code distorted terms. This will become apparent in the analysis of the Format B Decoder.

An important element of the Carrier Reconstruction Loop is the quadrupling circuit described in Appendix A.

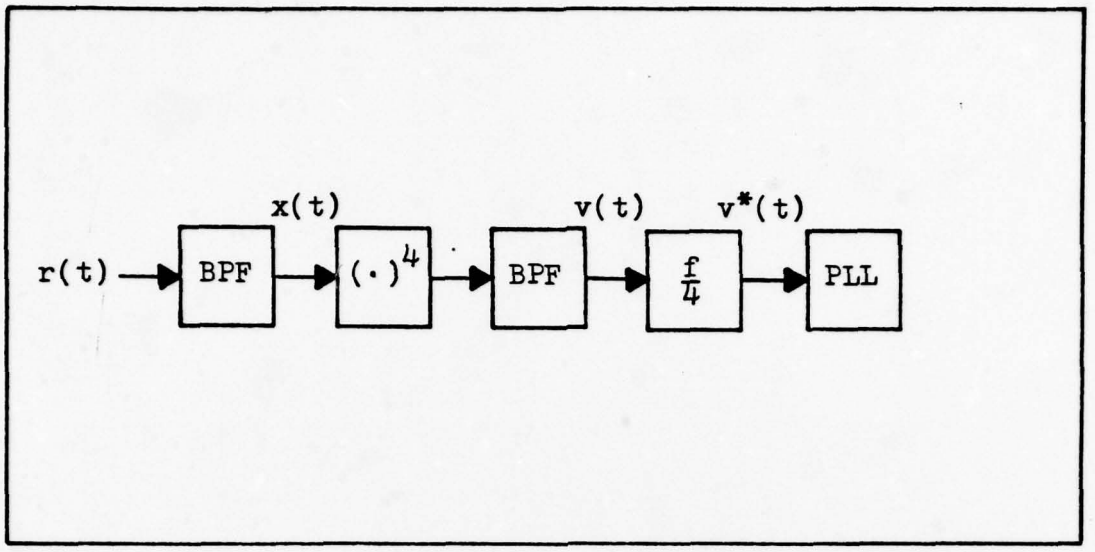


Figure 11. Carrier Reconstruction Loop.

It is shown in the appendix that the quadrupling circuit produces a signal at its output given by

$$
\begin{aligned}
v(t) = &\left[\frac{A^4}{8} p^4(t-nT_c) + \frac{A^4}{8} p^4(t-nT_c-T_c/2)\right. \\
&\left. - \frac{3}{4}A^4 p^2(t-nT_c)\, p^2(t-nT_c-T_c/2)\right] \\
&\cdot \cos[4\omega_0 t + 4\varphi(t)] \\
&+\left[\frac{A^4}{2} a_n b_n p^3(t-nT_c)\, p(t-nT_c-T_c/2)\right. \\
&\left. - \frac{A^4}{2} a_n b_n p(t-nT_c)\, p^3(t-nT_c-T_c/2)\right] \\
&\cdot \sin[4\omega_0 t + 4\varphi(t)] \\
&+ N_c(t) \cos[4\omega_0 t + 4\varphi(t)] \\
&+ N_s(t) \sin[4\omega_0 t + 4\varphi(t)] \qquad (53)
\end{aligned}
$$

where $N_c(t)$ and $N_s(t)$ are noise terms defined in Appendix A. If the "signal" component of $v(t)$ is defined to be the terms near $4\omega_0$ not multiplied by quadrature noise terms, then the

"signal" component at the output of the quadrupling circuit for the cases of O-QPSK, MSK, and SFSK pulse shaping are given by

$$S_{O\text{-}QPSK} = -\frac{A^4}{8}\cos[4\omega_0 t + 4\varphi(t)] \tag{54}$$

$$S_{MSK} = \frac{3}{64}A^4\cos[4\omega_0 t + 4\varphi(t)] \tag{55}$$

$$S_{SFSK} = \left[\frac{3}{64}A^4 + \frac{5}{64}A^4 J_1(1)\right]\cos[4\omega_0 t + 4\varphi(t)] \tag{56}$$

where $J_1(1)$ is the Bessel function of the first kind of order 1 and with argument 1. Thus, regardless of the pulse shaping used by the transmitter, for the generic modulation formats considered here the output of the quadrupling circuit can always be expressed as

$$\begin{aligned} v(t) = &-V\cos[4\omega_0 t + 4\varphi(t)] \\ &+ N_c(t)\cos[4\omega_0 t + 4\varphi(t)] \\ &+ N_s(t)\sin[4\omega_0 t + 4\varphi(t)] \end{aligned} \tag{57}$$

This result is divided in frequency by four to give

$$\begin{aligned} v^*(t) = &[-V + N_c(t)]\cos[\omega_0 t + \varphi(t)] \\ &+ N_s(t)\sin[\omega_0 t + \varphi(t)] \end{aligned} \tag{58}$$

This signal, then, is presented to the Format B Decoder and the PLL. As is demonstrated in Appendix A, the signal to noise ratio (SNR) is typically quite large here, and hence the noise contributions are negligible. Then for all cases of interest, a trackable signal is presented to the PLL and

coherent reference signals at the carrier frequency can be produced. Also, the Format B Decoder is given a signal containing the modulation terms (in the case of modulation format B) that is free of PN code terms and significant noise terms.

With coherent carrier reference signals available, the intercept receiver is able to decode transmissions from both modulations format A and B. The first of these to be considered will be format A.

Format A Decoder. The Format A Decoder is shown again in Figure 12. Here, the signals in the in-phase and quadrature channels will be calculated. Outputs will be calculated for O-QPSK, MSK, and SFSK pulse shaping of the data. It will be shown that when only one transmission is received, message decoding is not possible at the channel outputs. However, when two messages from different transmitters are received simultaneously, it will be shown that it is possible to decode both messages if the transmissions arrive at the receiver within the same PN code bit interval (i.e., the transmitters are synchronized and approximately equal distances from the receiver).

When one transmission is received the input to the decoder is given by equation (50), repeated here.

$$x(t) = [Aa_n p(t-nT_c) + n_c(t)] \cos[\omega_0 t + \varphi(t)] + [Ab_n p(t-nT_c-T_c/2) - n_s(t)] \sin[\omega_0 t + \varphi(t)] \quad (50)$$

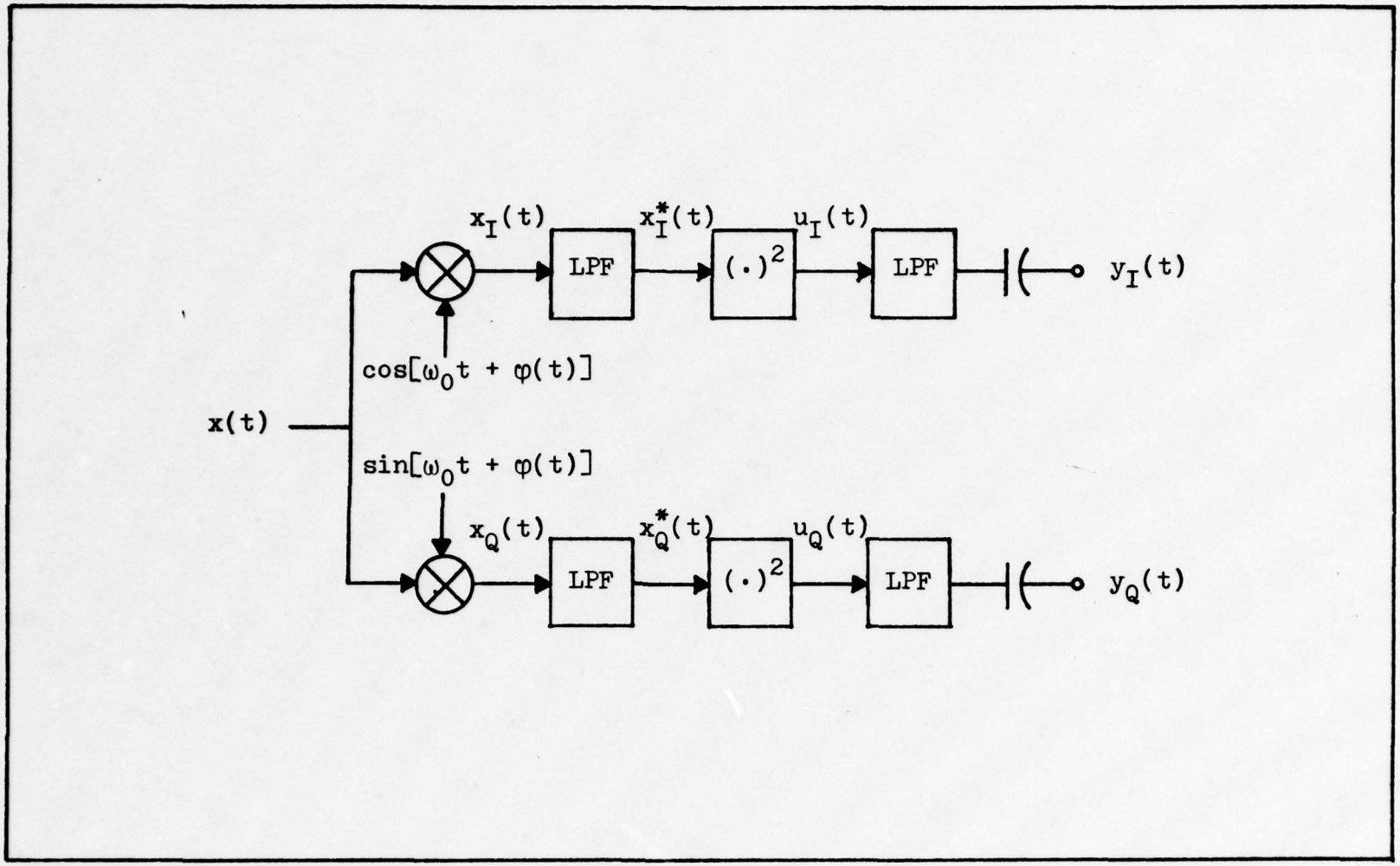


Figure 12. Format A Decoder.

This signal is mixed with coherent reference signals in the in-phase and quadrature channels to produce

$$x_I(t) = \frac{A}{2}a_n p(t-nT_c) + \frac{1}{2}n_c(t) + \left[\frac{A}{2}a_n p(t-nT_c) + \frac{1}{2}n_c(t)\right]\cos[2\omega_0 t + 2\varphi(t)] + \left[\frac{A}{2}b_n p(t-nT_c-T_c/2) - \frac{1}{2}n_s(t)\right]\sin[2\omega_0 t + 2\varphi(t)] \quad (59)$$

and

$$x_Q(t) = \frac{A}{2}b_n p(t-nT_c-T_c/2) - \frac{1}{2}n_s(t) - \left[\frac{A}{2}b_n p(t-nT_c-T_c/2) - \frac{1}{2}n_s(t)\right]\cos[2\omega_0 t + 2\varphi(t)] + \left[\frac{A}{2}a_n p(t-nT_c) + \frac{1}{2}n_c(t)\right]\sin[2\omega_0 t + 2\varphi(t)] \quad (60)$$

These signals are filtered thru ideal low pass filters (LPF) with BW = B, the transmission bandwidth. Because the carrier frequency is much larger than the transmission bandwidth, only the first two terms in each equation are passed. The output of the filters is then:

$$x_I^*(t) = \frac{A}{2}a_n p(t-nT_c) + \frac{1}{2}n_c(t) \quad (61)$$

$$x_Q^*(t) = \frac{A}{2}b_n p(t-nT_c-T_c/2) - \frac{1}{2}n_s(t) \quad (62)$$

The signals are now processed thru square law devices to produce signal terms independent of coding. Recalling that $a_n^2 = b_n^2 = 1$, the output of the square law devices is:

$$u_I(t) = \frac{A^2}{4}p^2(t-nT_c) + \frac{1}{4}n_c^2(t) + \frac{A}{2}a_n p(t-nT_c)n_c(t) \quad (63)$$

$$u_Q(t) = \frac{A^2}{4} p^2(t-nT_c-T_c/2) + \frac{1}{4}n_s^2(t) - \frac{A}{2}b_n p(t-nT_c-T_c/2)n_s(t) \quad (64)$$

At this point, it is necessary to include the specific pulse shaping functions. Using equations (33), (34) and (35) in (63) and (64), the output of the square law device for O-QPSK, MSK, and SFSK pulse shaping is as follows. For O-QPSK:

$$u_I(t) = \frac{A^2}{4} + \frac{1}{4}n_c^2(t) + \frac{A}{2}a_n n_c(t) \quad (65)$$

$$u_Q(t) = \frac{A^2}{4} + \frac{1}{4}n_s^2(t) - \frac{A}{2}b_n n_s(t) \quad (66)$$

For MSK pulse shaping:

$$u_I(t) = \frac{A^2}{8} + \frac{A^2}{8}\cos\left(\frac{2\pi t}{T_c}\right) + \frac{A}{2}a_n \cos\left(\frac{\pi t}{T_c}\right)n_c(t) + \frac{1}{4}n_s^2(t) \quad (67)$$

$$u_Q(t) = \frac{A^2}{8} - \frac{A^2}{8}\cos\left(\frac{2\pi t}{T_c}\right) - \frac{A}{2}b_n \sin\left(\frac{\pi t}{T_c}\right)n_s(t) + \frac{1}{4}n_s^2(t) \quad (68)$$

The output of the quadrupler for SFSK pulse shaping is more difficult to evaluate, so intermediate steps will be included here. In this case

$$u_I(t) = \frac{A^2}{4}\cos^2\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\left(\frac{4\pi t}{T_c}\right)\right]$$

$$+ \frac{A}{2}a_n \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\left(\frac{4\pi t}{T_c}\right)\right] n_c(t) + \frac{1}{4}n_c^2(t)$$

$$= \frac{A^2}{8} + \frac{A^2}{8}\cos\left[\frac{2\pi t}{T_c} - \frac{1}{2}\sin\left(\frac{4\pi t}{T_c}\right)\right]$$

$$+ \frac{A}{2}a_n \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\left(\frac{4\pi t}{T_c}\right)\right] n_c(t) + \frac{1}{4}n_c^2(t)$$

$$= \frac{A^2}{8} + \frac{A^2}{8}\sum_n J_n(1/2)\cos\left[(1-2n)\frac{2\pi t}{T_c}\right]$$

$$+ \frac{A}{2}a_n \sum_n J_n(1/4)\cos\left[(1-4n)\frac{\pi t}{T_c}\right] n_c(t) + \frac{1}{4}n_c^2(t) \qquad (69)$$

where $J_n(\mu)$ is the n^{th} order Bessel function of the first kind with argument μ, and where (Ref. 22:116)

$$\nu \cos[\omega_0 t + (\mu)\sin(\omega_m t] = \nu \sum_n J_n(\mu)\cos[(\omega_c + n\omega_m)t] \qquad (70)$$

The output of the square law device in the quadrature channel for SFSK pulse shaping is, similarly

$$u_Q(t) = \frac{A^2}{8} - \frac{A^2}{8}\sum_n J_n(1/2)\cos\left[(1-2n)\frac{2\pi t}{T_c}\right]$$

$$- \frac{A}{2}b_n \sum_n J_n(1/4)\sin\left[(1-4n)\frac{\pi t}{T_c}\right] n_s(t) + \frac{1}{4}n_s^2(t) \qquad (71)$$

Before stating the outputs of the Format A Decoder, it is necessary to consider the effect of the final LPF. This ideal filter has a bandwidth W on the order of the reciprocal of the sampling rate at the transmitter ($W \approx 1/T$), the information bandwidth. If the PSD and autocorrelation function of the output were of interest, then it would be appropriate to compute these characteristics at the input to this filter at this time and derive the equivalent expressions for the output. However, determining the output in

the time domain from the output autocorrelation function is not possible. For example, two PN codes have the same autocorrelation function, but their time history can be completely different. Since a time domain expression for the output is of primary importance here, the following representation be used to describe the portion of the signal passed by the ideal low pass filter: $[\ ]_{LP}$.

The output of the Format A Decoder for the different pulse shaping functions when one transmission is received, then, is as follows. For O-QPSK:

$$y_I(t) = \left[\frac{1}{4}n_c^2(t) + \frac{A}{2}a_n n_c(t)\right]_{LP} \tag{72}$$

$$y_Q(t) = \left[\frac{1}{4}n_s^2(t) - \frac{A}{2}b_n n_s(t)\right]_{LP} \tag{73}$$

For MSK:

$$y_I(t) = \left[\frac{1}{4}n_c^2(t)\right]_{LP} \tag{74}$$

$$y_Q(t) = \left[\frac{1}{4}n_s^2(t)\right]_{LP} \tag{75}$$

For SFSK:

$$y_I(t) = \left[\frac{1}{4}n_c^2(t)\right]_{LP} \tag{76}$$

$$y_Q(t) = \left[\frac{1}{4}n_s^2(t)\right]_{LP} \tag{77}$$

Recall now that for modulation format A, a_n and b_n are composed of modulation terms and code terms. Notice in the output, equations (72) thru (77), that there are only noise terms or coded modulation terms multiplied by noise. Thus, it is clear that for the case where only one transmission is received, no information can be recovered at the

output. However, it will now be shown that for the case where two simultaneous transmissions are received by the interceptor that arrive within the same PN code bit interval, message reconstruction is possible.

Consider the received waveform for two simultaneous transmissions. A PN code bit offset of $\Delta t < T_c$ will be assumed in the analysis. A carrier phase difference of Φ will be assumed between transmitter 1 and transmitter 2, also. The received waveform for the interval $nT_c < t < nT_c + T_c/2$ is

$$\begin{aligned} r(t) = {} & A_1 a_{n1} p(t-nT_c) \cos(\omega_0 t) \\ & + A_1 b_{n1} p(t-nT_c-T_c/2) \sin(\omega_0 t) \\ & + A_2 a_{n2} p(t-nT_c-\Delta t) \cos(\omega_0 t + \Phi) \\ & + A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t) \sin(\omega_0 t + \Phi) \\ & + n(t) \end{aligned} \tag{78}$$

where the subscripts 1 and 2 refer to the contributions from transmitters 1 and 2. With $\alpha = \cos \Phi$ and $\beta = \sin \Phi$, the signal at the output of the front end filter is

$$\begin{aligned} x(t) = {} & [A_1 a_{n1} p(t-nT_c) + \alpha A_2 a_{n2} p(t-nT_c - \Delta t) \\ & + \beta A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t)] \cos(\omega_0 t) \\ & + [A_1 b_{n1} p(t-nT_c-T_c/2) + \alpha A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t) \\ & - \beta A_2 a_{n2} p(t-nT_c-\Delta t) - n_s(t)] \sin(\omega_0 t) \end{aligned} \tag{79}$$

The calculations necessary to compute the outputs become quite lengthy and complicated at this point, hence, they have been included in Appendix B. The outputs of the Format A Decoder for two simultaneous transmissions are listed as

follows. For O-QPSK pulse shaping:

$$y_I(t) = \frac{\alpha}{2}A_1A_2a_{n1}a_{n2} + \left[\frac{\beta}{2}A_1A_2a_{n1}a_{n2}\right]_{LP} + \left[\frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\right]_{LP} + \left[\frac{1}{4}n_c^2(t)\right]_{LP} + \left[\left(\frac{1}{2}A_1a_{n1} + \frac{\alpha}{2}A_2a_{n2} + \frac{\beta}{2}A_2a_{n2}\right)n_c(t)\right]_{LP} \quad (80)$$

$$y_Q(t) = \frac{\alpha}{2}A_1A_2b_{n1}b_{n2} - \left[\frac{\beta}{2}A_1A_2a_{n2}b_{n1}\right]_{LP} - \left[\frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\right]_{LP} + \left[\frac{1}{4}n_s^2(t)\right]_{LP} - \left[\left(\frac{1}{2}A_1b_{n1} + \frac{\alpha}{2}A_2b_{n2} + \frac{\beta}{2}A_2a_{n2}\right)n_s(t)\right]_{LP} \quad (81)$$

For MSK pulse shaping, the outputs are:

$$y_I(t) = \frac{\alpha}{4}A_1A_2a_{n1}a_{n2}\cos\left(\frac{\pi\Delta t}{T_c}\right) - \left[\frac{\beta}{4}A_1A_2a_{n1}b_{n2}\sin\left(\frac{\pi\Delta t}{T_c}\right)\right]_{LP} + \left[\frac{1}{4}n_c^2(t)\right]_{LP} \quad (82)$$

$$y_Q(t) = \frac{\alpha}{4}A_1A_2b_{n1}b_{n2}\cos\left(\frac{\pi\Delta t}{T_c}\right) + \left[\frac{\beta}{4}A_1A_2a_{n2}b_{n1}\sin\left(\frac{\pi\Delta t}{T_c}\right)\right]_{LP} + \left[\frac{1}{4}n_s^2(t)\right]_{LP} \quad (83)$$

The corresponding terms for SFSK pulse shaping are:

$$y_I(t) = \frac{\alpha}{4}A_1A_2a_{n1}a_{n2}\cos\left(\frac{\pi\Delta t}{T_c}\right)J_0^2(1/4) - \left[\frac{\beta}{4}A_1A_2a_{n2}b_{n1}\sin\left(\frac{\pi\Delta t}{T_c}\right)J_0^2(1/4)\right]_{LP} + \left[\frac{1}{4}n_c^2(t)\right]_{LP} \quad (84)$$

$$y_Q(t) = \frac{\alpha}{4}A_1A_2b_{n1}b_{n2}\cos\left(\frac{\pi\Delta t}{T_c}\right)J_0^2(1/4) + \left[\frac{\beta}{4}A_1A_2a_{n2}b_{n1}\sin\left(\frac{\pi\Delta t}{T_c}\right)J_0^2(1/4)\right]_{LP} + \left[\frac{1}{4}n_s^2(t)\right]_{LP} \quad (85)$$

Before proceeding further in the developement, it is instructive to examine the output equations in detail. First consider what the interceptor is looking for: terms that contain the information but are free of PN code terms and are not multiplied by noise. For modulation format A, recall that $a_{n1} = c_{In}d_{In1}$, $a_{n2} = c_{In}d_{In2}$, $b_{n1} = c_{Qn}d_{Qn1}$, and $b_{n2} = c_{Qn}d_{Qn2}$ where the "c" terms are PN code terms, the "d" terms are the desired data or information, and where the numeric subscripts refer to transmitter 1 and 2 [see definitions under equation (40)]. These terms appear in the output equations in the following combinations:

$$a_{n1}a_{n2} = d_{In1}d_{In2} \tag{86}$$

$$a_{n1}b_{n2} = c_{In}c_{Qn}d_{In1}d_{Qn2} \tag{87}$$

$$a_{n2}b_{n1} = c_{In}c_{Qn}d_{In2}d_{Qn1} \tag{88}$$

$$a_{n2}b_{n2} = c_{In}c_{Qn}d_{In2}d_{Qn2} \tag{89}$$

$$b_{n1}b_{n2} = d_{Qn1}d_{Qn2} \tag{90}$$

The code-free terms are thus the ones that contain either $a_{n1}\cdot a_{n2}$ or $b_{n1}\cdot b_{n2}$. Then the first term of each of the Format A Decoder output equations, equations (80) thru (85), is the desired term from which the interceptor would try to reconstruct the message.

Also notice in the output equations that the transmitter's relative carrier phase offsets and the PN code bit offset play a major role in the relative amplitudes of the

terms. The terms containing code have a PSD that is low compared to the terms without code, so it can be argued heuristically that they remain at a relatively low and approximately constant power. Thus, the amplitude of the first term is of primary importance in its detection.

Consider now the ideal case where the carriers arrive in phase, the PN code bits exactly coincide, and the noise power is negligible. This corresponds to $\alpha = 1$, $\beta = 0$, $\Delta t = 0$, and $n_s(t) = n_c(t) = 0$. The decoder outputs under these ideal conditions are given in Table I. These same results are duplicated in Table II except that the substitutions for the "a" and "b" terms have been made, and the "n" subscript has been dropped since it only indicates that the results are for the n^{th} interval. Examination of Table II shows that regardless of the pulse shaping used, the output of the receiver contains the essential speech ingredients multiplied by a constant.

How, then, is the message reconstructed from these outputs? First, it is assumed that the outputs are normalized by some gain control circuity so that the output in each case is

$$y_I(t) = d_{I1}d_{I2} \tag{91}$$

and

$$y_Q(t) = d_{Q1}d_{Q2} \tag{92}$$

Keep in mind that filtering the output had the effect of integrating over the sample period, T. The above equation

TABLE I

Format A Decoder Output
Under Ideal Conditions.
General Waveform Case.

Pulse Shaping	$y_I(t)$	$y_Q(t)$
O-QPSK	$\frac{1}{2}A_1A_2a_{n1}a_{n2}$	$\frac{1}{2}A_1A_2b_{n1}b_{n2}$
MSK	$\frac{1}{4}A_1A_2a_{n1}a_{n2}$	$\frac{1}{4}A_1A_2b_{n1}b_{n2}$
SFSK	$\frac{1}{4}A_1A_2a_{n1}a_{n2}J_0^2(1/4)$	$\frac{1}{4}A_1A_2b_{n1}b_{n2}J_0^2(1/4)$

TABLE II

Format A Decoder Output
Under Ideal Conditions.
Modulation Format A Case.

Pulse Shaping	$y_I(t)$	$y_Q(t)$
O-QPSK	$\frac{1}{2}A_1A_2d_{I1}d_{I2}$	$\frac{1}{2}A_1A_2d_{Q1}d_{Q2}$
MSK	$\frac{1}{4}A_1A_2d_{I1}d_{I2}$	$\frac{1}{4}A_1A_2d_{Q1}d_{Q2}$
SFSK	$\frac{1}{4}A_1A_2d_{I1}d_{I2}J_0^2(1/4)$	$\frac{1}{4}A_1A_2d_{Q1}d_{Q2}J_0^2(1/4)$

is the output over ove PN code chip interval, T_c. The output over all time is

$$y_I(t) = d_{I1}(t)d_{I2}(t) \tag{93}$$

$$y_Q(t) = d_{Q1}(t)d_{Q2}(t) \tag{94}$$

Let $d_1(t)$ and $d_2(t)$ be the waveforms at the output of the pulse width modulators of transmitters 1 and 2 respectively (see Figure 7). Since $d_1(t)$ and $d_2(t)$ can over any sample interval represent a positive, negative, or zero sample, then there are nine cases which must be considered.

1) $d_1(t)$ positive
   $d_2(t)$ positive

2) $d_1(t)$ positive
   $d_2(t)$ negative

3) $d_1(t)$ negative
   $d_2(t)$ positive

4) $d_1(t)$ negative
   $d_2(t)$ negative

5) $d_1(t)$ positive
   $d_2(t)$ zero

6) $d_1(t)$ negative
   $d_2(t)$ zero

7) $d_1(t)$ zero
   $d_2(t)$ positive

8) $d_1(t)$ zero
   $d_2(t)$ negative

9) $d_1(t)$ zero
   $d_2(t)$ zero

Each of the nine cases is illustrated in Figure 13.a thru 13.i. Consider case 2, Figure 13.b, where $d_1(t)$ represents a positive sample and $d_2(t)$ represents a negative sample.[5] Here, and in all nine cases, τ_1 and τ_2 represent

[5]The reader is encouraged to review the Generic Modulation Format A section of chapter III for clarification of this development.

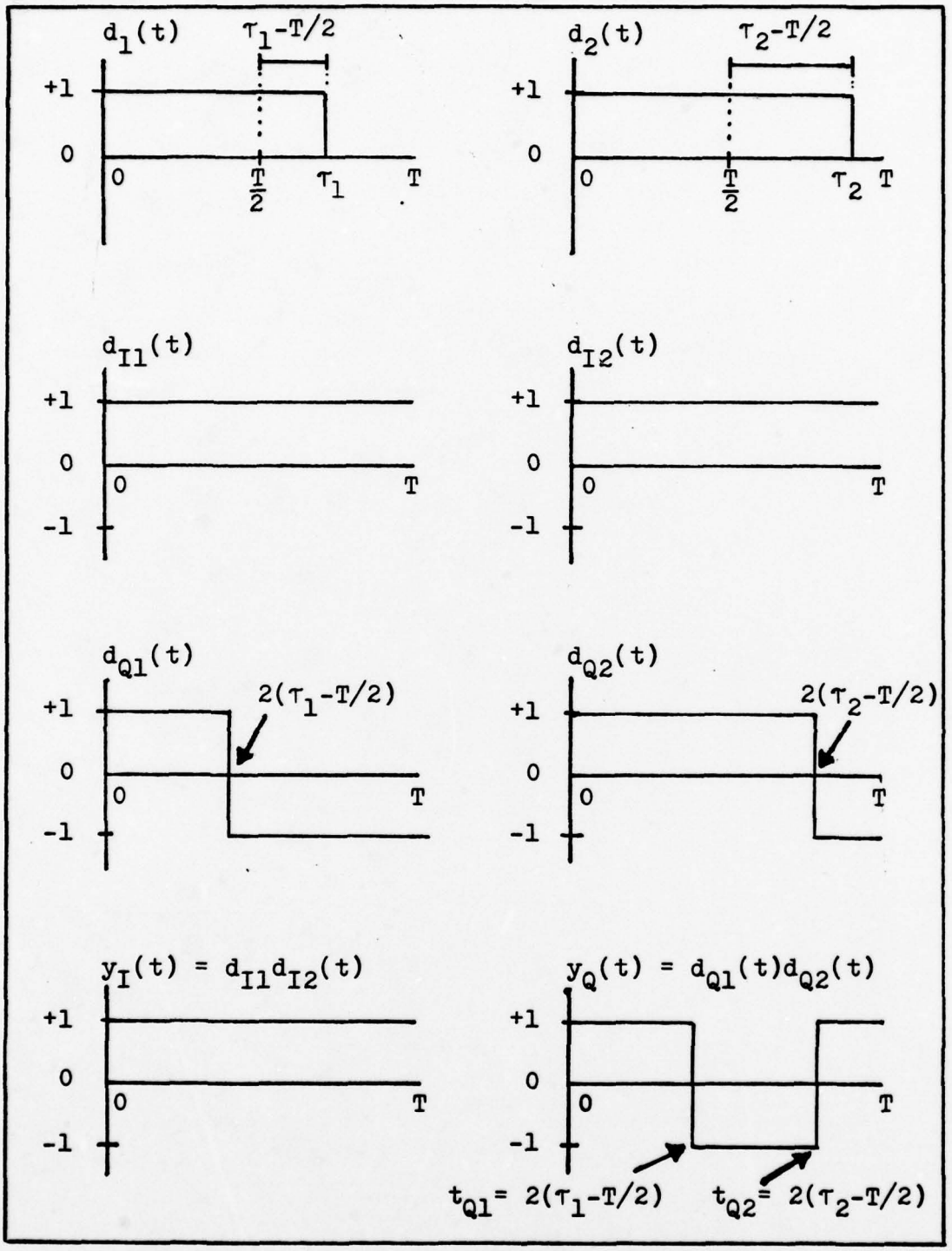


Figure 13.a. Data Signals and Format A Decoder Outputs - Case 1.

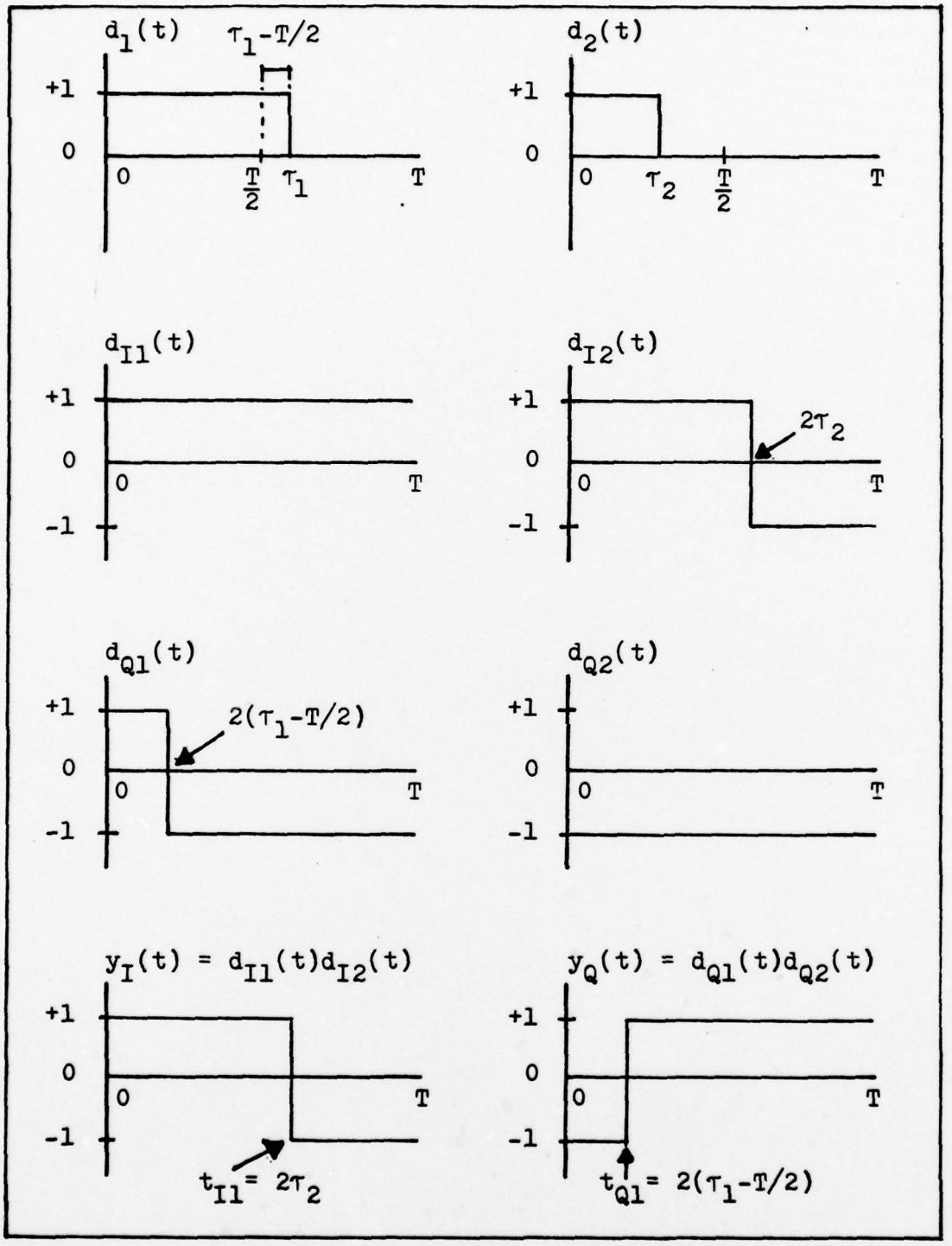


Figure 13.b. Data Signals and Format A Decoder Outputs - Case 2.

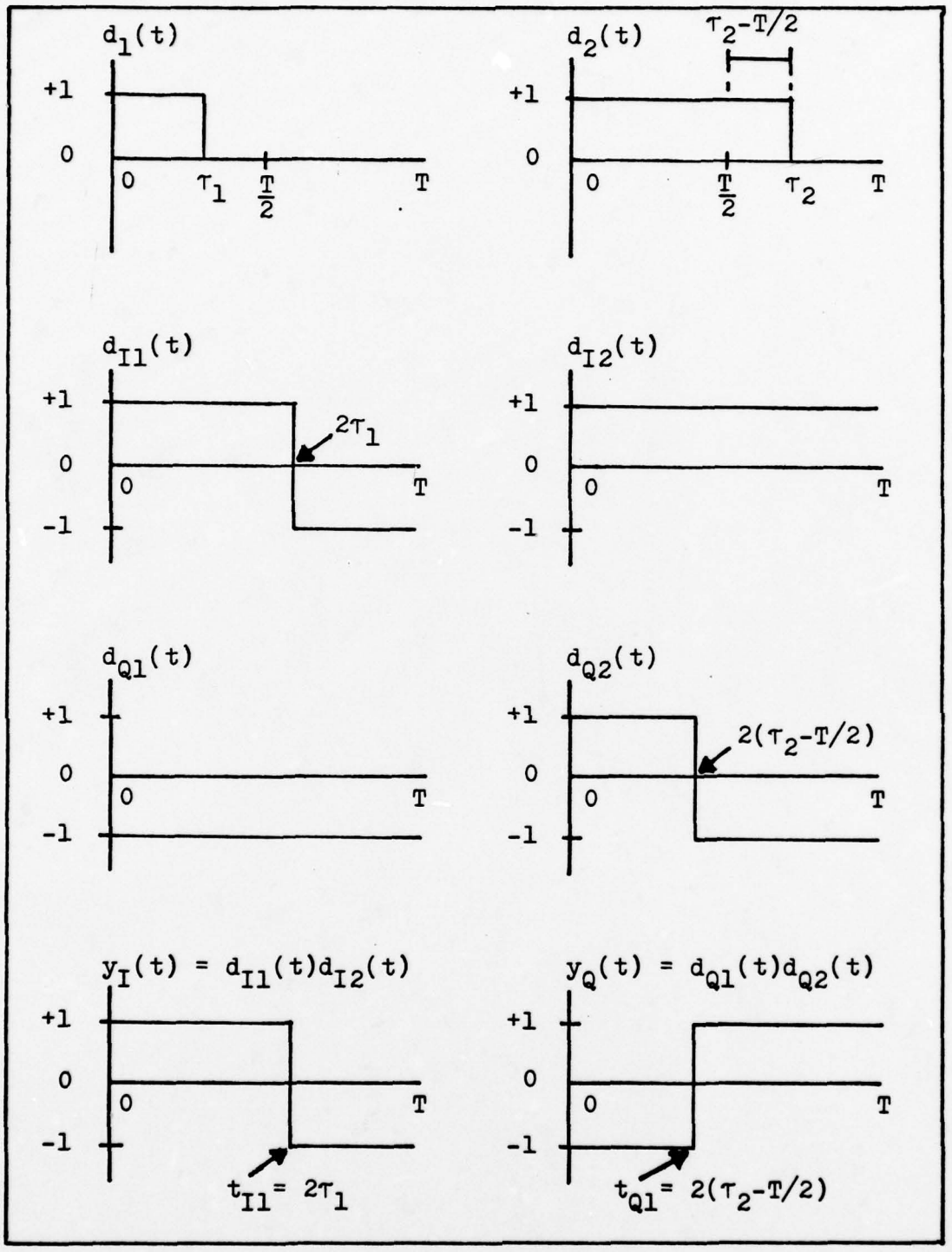


Figure 13.c. Data Signals and Format A Decoder Outputs - Case 3.

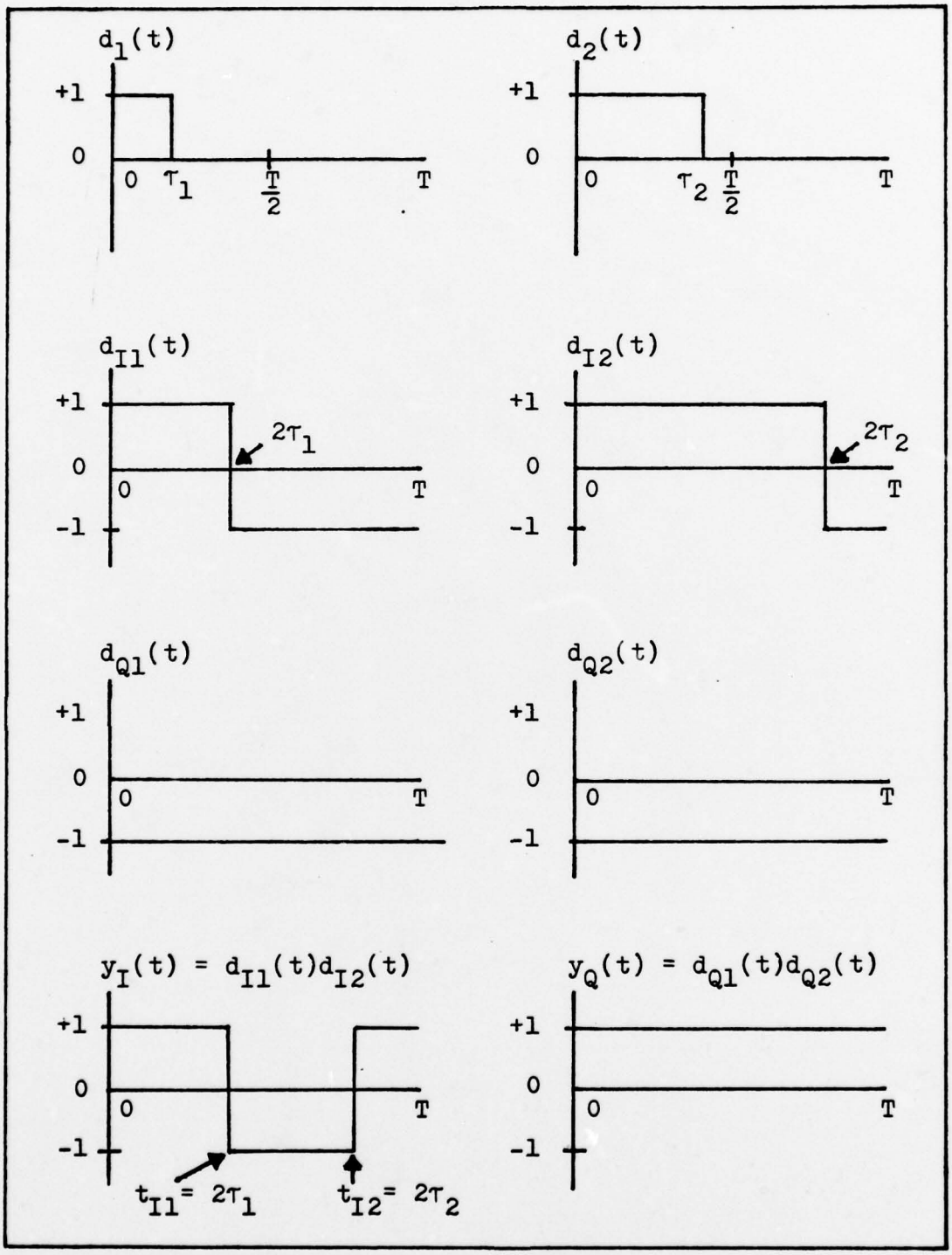


Figure 13.d. Data Signals and Format A Decoder Outputs - Case 4.

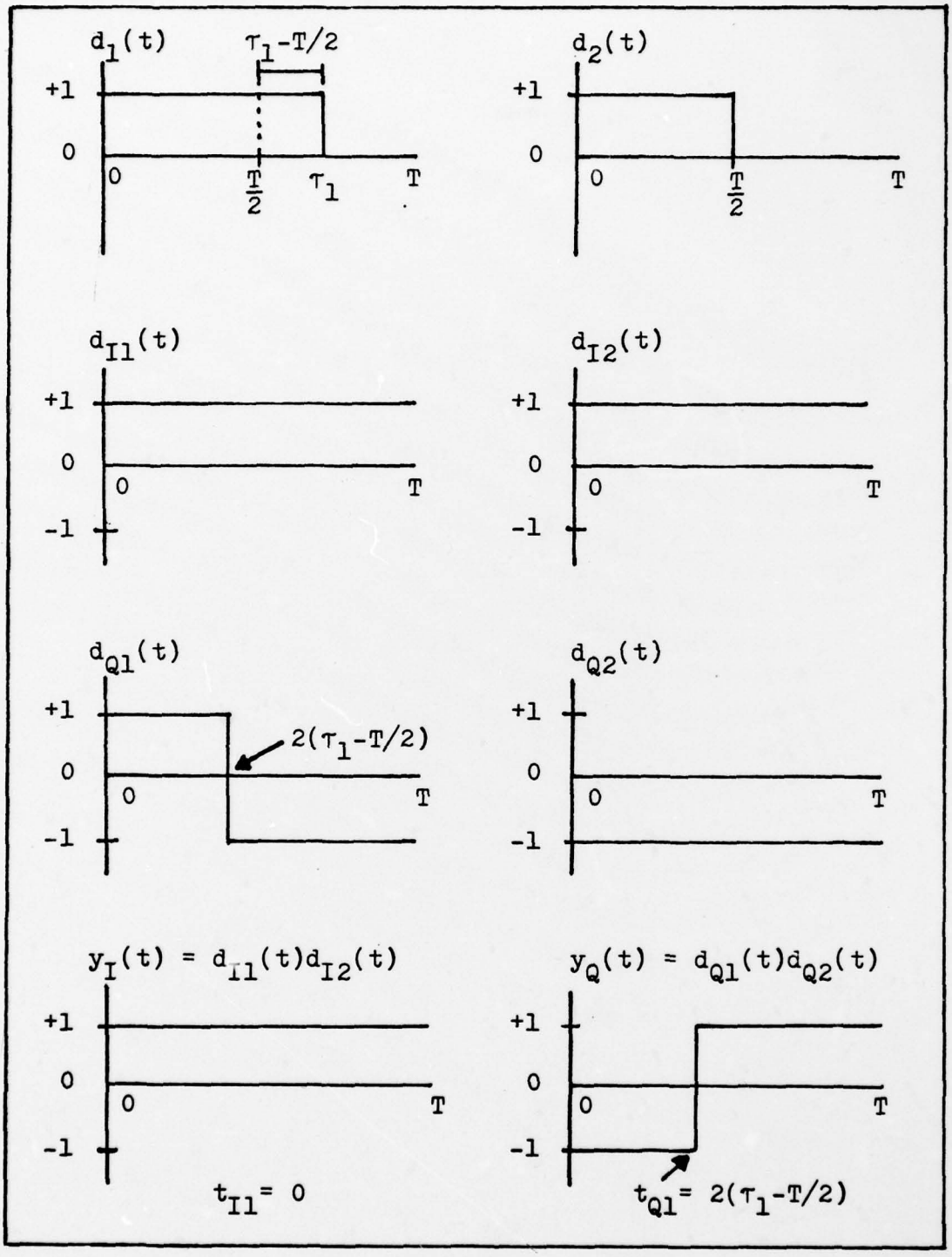


Figure 13.e. Data Signals and Format A Decoder Outputs - Case 5.

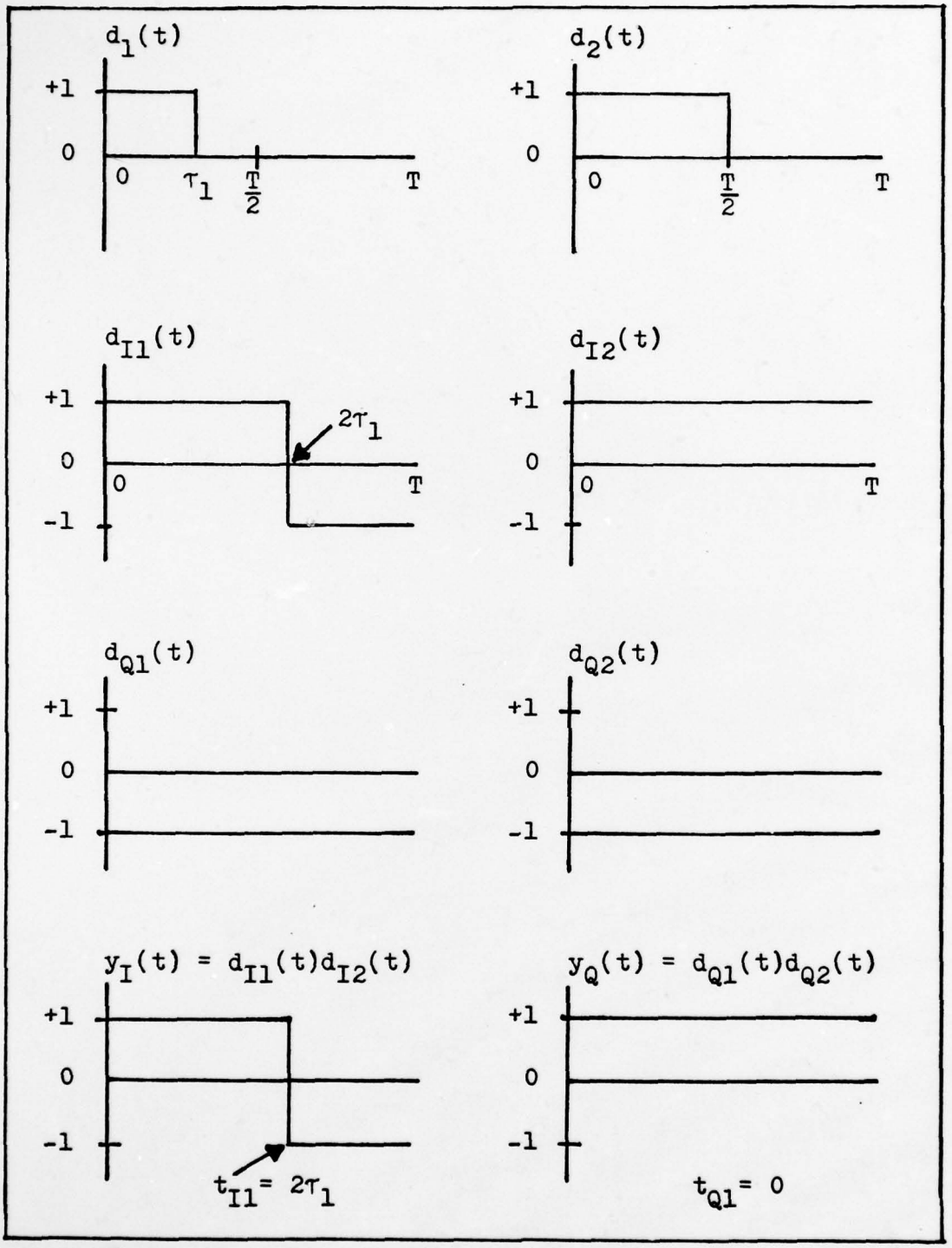


Figure 13.f. Data Signals and Format A Decoder Outputs - Case 6.

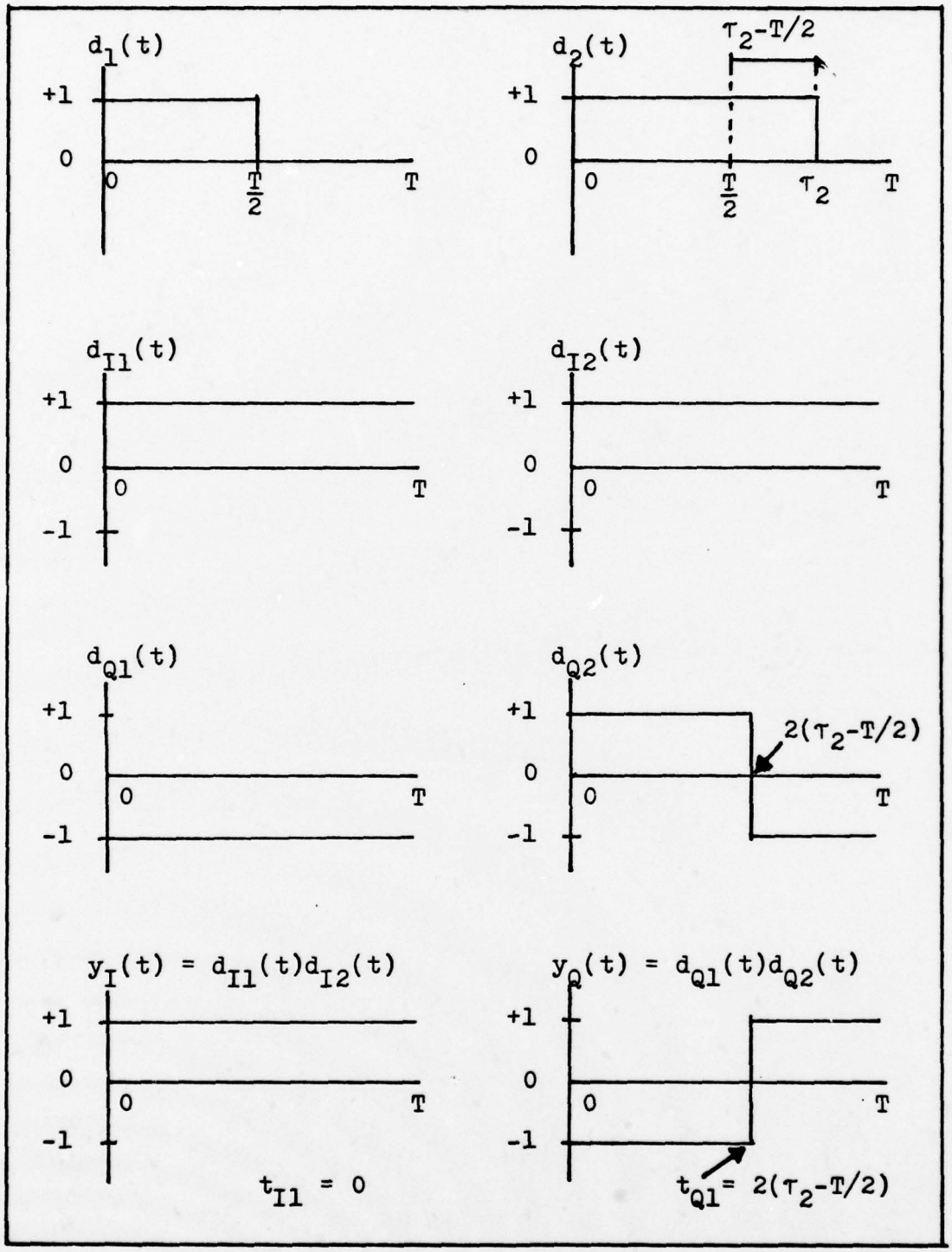


Figure 13.g. Data Signals and Format A Decoder Outputs - Case 7.

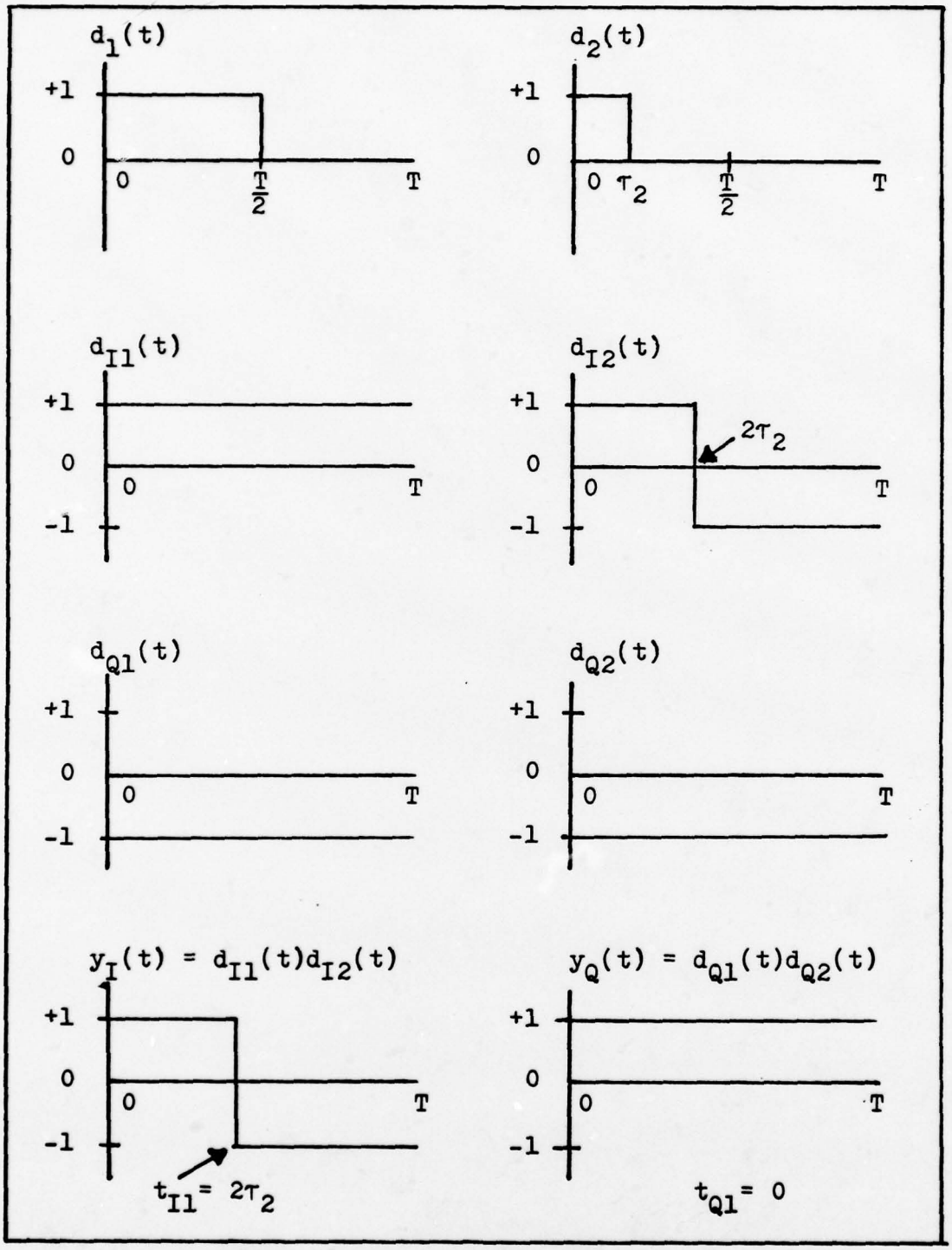


Figure 13.h. Data Signals and Format A Decoder Outputs - Case 8.

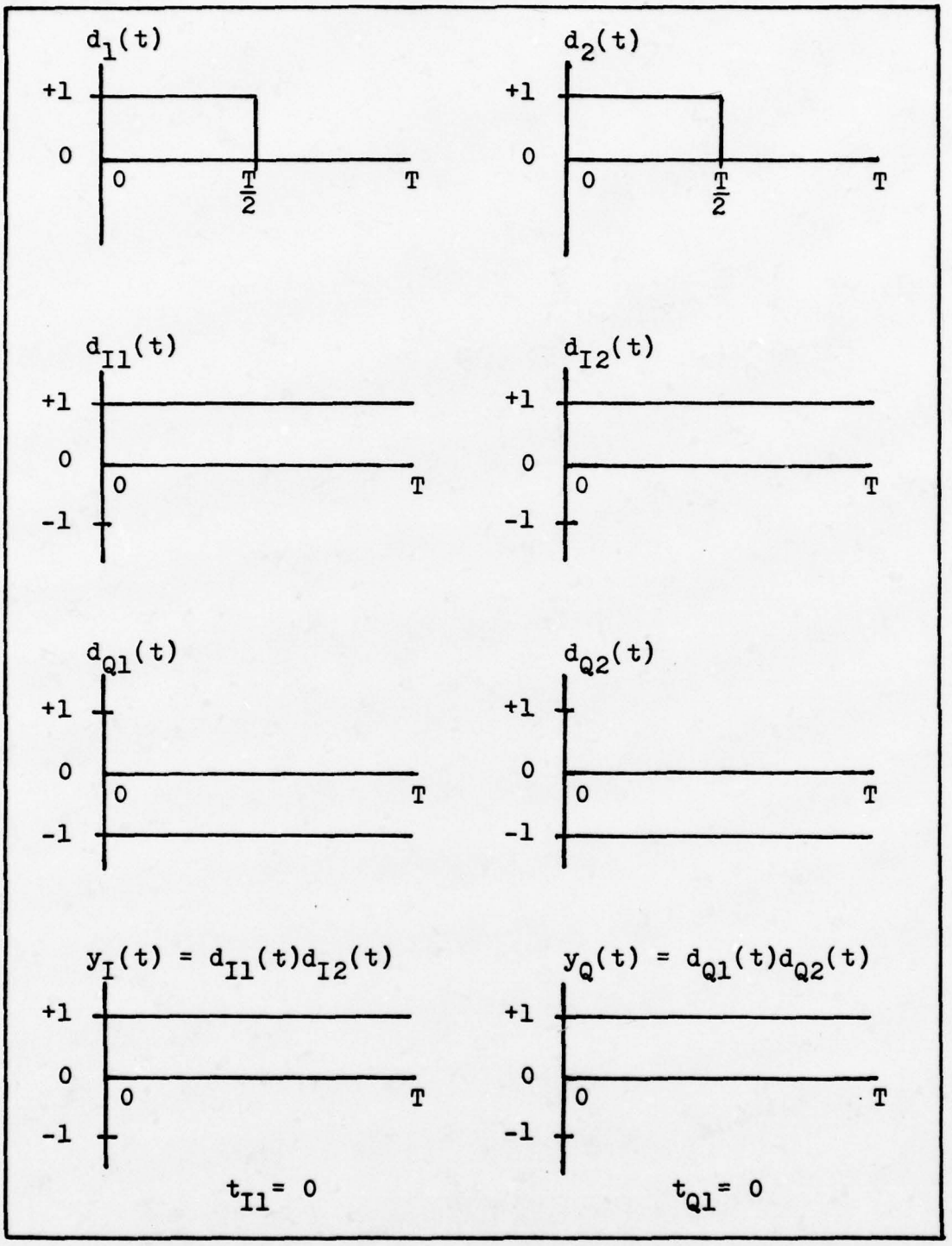


Figure 13.i. Data Signals and Format A Decoder Outputs - Case 9.

the pulse widths of $d_1(t)$ and $d_2(t)$ respectively over one sample interval of duration T. Notice that $d_1(t)$ has been divided into two sections of duration T/2. The first section has a constant value over the interval, so it can be represented by a pulse of width T/2. This pulse width is doubled and routed to the in-phase channel at the transmitter to produce the signal $d_{I1}(t)$. Similarly, the second section of $d_1(t)$ can be represented by a pulse of width τ_1-T/2. This also is doubled in width and routed to the quadrature phase channel of the transmitter to produce the signal $d_{Q1}(t)$. The signals $d_{I2}(t)$ and $d_{Q2}(t)$ are derived from $d_2(t)$ in identical fashion. The figure also shows the outputs of the receiver, $y_I(t)$ and $y_Q(t)$, as given by equations (93) and (94). By a similar treatment, the outputs are developed for the remaining eight cases.

From equation (37), it is clear that the pulse widths, τ_1 and τ_2, of the message sample values, m_{k1} and m_{k2}, are related by the following:

$$\tau_1 = (1+m_{k1})T/2 \tag{95}$$

$$\tau_2 = (1+m_{k2})T/2 \tag{96}$$

Then the message sample values are:

$$m_{k1} = 2\tau_1/T - 1 \tag{97}$$

$$m_{k2} = 2\tau_2/T - 1 \tag{98}$$

Thus, to recover the message samples, τ_1 and τ_2 must be determined from the outputs of the receiver, $y_I(t)$ and $y_Q(t)$.

One way that the interceptor might proceed is to try to recover m_{k1} and m_{k2} independently of each other, so he must come up with some decoding rule to accomplish this. Notice that for any particular case, the output may contain zero, one, or two zero crossings in the sample interval. The times to the first and second zero crossing (if any) in $y_I(t)$ are designated as t_{I1} and t_{I2}, respectively. In $y_Q(t)$, these are designated as t_{Q1} and t_{Q2}. It should be clear that the interceptor can not know whether a particular zero crossing is caused by transmitter 1 or 2. Therefore he must make some assumption. He assumes, rightly or wrongly, that when only one crossing occurs in $y_I(t)$, it is caused by transmitter 1, and when only one occurs in $y_Q(t)$ that it is caused by transmitter 2. When two zero crossings occur in $y_I(t)$, the first is assumed to be caused by transmitter 1 and the second by transmitter 2. In $y_Q(t)$, the first is assumed caused by transmitter 2 and the second by transmitter 1. To summarize:

$$t_{I1} \rightarrow \text{transmitter 1 } (\hat{\tau}_1)$$
$$t_{I2} \rightarrow \text{transmitter 2 } (\hat{\tau}_2)$$
$$t_{Q1} \rightarrow \text{transmitter 2 } (\hat{\tau}_2)$$
$$t_{Q2} \rightarrow \text{transmitter 1 } (\hat{\tau}_1)$$

Under the above assumptions, the following estimates of τ_1 and τ_2 can be made. From the in-phase channel ($y_I(t)$):

$$\hat{\tau}_1 = t_{I1}/2 \tag{99}$$

$$\hat{\tau}_2 = t_{I2}/2 \tag{100}$$

From the quadrature channel ($y_Q(t)$):

$$\hat{\tau}_1 = (t_{Q2} + T)/2 \tag{101}$$

$$\hat{\tau}_2 = (t_{Q1} + T)/2 \tag{102}$$

Using these estimates in equations (97) and (98) gives the following decoding rules. For the in-phase channel ($y_I(t)$):

$$\hat{m}_{k1} = t_{I1}/T - 1 \tag{103}$$

$$\hat{m}_{k2} = t_{I2}/T - 1 \tag{104}$$

For the quadrature channel ($y_Q(t)$):

$$\hat{m}_{k1} = t_{Q2}/T \tag{105}$$

$$\hat{m}_{k2} = t_{Q2}/T \tag{106}$$

When only one transition occurs in either channel, the rule is

$$\hat{m}_{k1} = t_{I1}/T - 1 \tag{107}$$

for the in-phase channel and

$$\hat{m}_{k2} = t_{Q1}/T - 1 \tag{108}$$

for the quadrature channel. The obvious flaw with this method is that on the average, this will result in a correct decision being made only fifty percent of the time since the interceptor can't know which transmitter caused which transition.

Since the human ear does a good job of discriminating simultaneous voices, a better scheme would be to determine

the sum of the message samples, $m_{k1} + m_{k2}$. In this case

$$m_{k1} + m_{k2} = 2(\tau_1+\tau_2)/T - 2 \tag{109}$$

The problem now becomes one of estimating $\tau_1+\tau_2$ instead of τ_1 and τ_2 individually.

Consider Case 1, Figure 13.a, where $d_1(t)$ and $d_2(t)$ both represent positive samples. At $y_Q(t)$, suppose that a wrong assumption is made: that t_{Q1} is caused by transmitter 2. Mathematically, the assumption is:

$$\hat{\tau}_1 = (t_{Q2} + T)/2 \tag{110}$$

$$\hat{\tau}_2 = (t_{Q1} + T)/2 \tag{111}$$

Then

$$\hat{\tau}_1 + \hat{\tau}_2 = (t_{Q1}+t_{Q2})/2 + T \tag{112}$$

In reality, t_{Q1} was caused by transmitter 1. Mathematically, this is:

$$\tau_1 = (t_{Q1} + T)/2 \tag{113}$$

$$\tau_2 = (t_{Q2} + T)/2 \tag{114}$$

Then

$$\tau_1 + \tau_2 = (t_{Q1}+t_{Q2})/2 + T = \hat{\tau}_1 + \hat{\tau}_2 \tag{115}$$

Thus, even though the wrong assumption was made, by adding the result, the sum of the samples can be reconstructed unambiguously on each sampling interval. This result occurs for each of the nine possible cases. In each case, the sum

of the two samples can be recovered without having to make an assumption about which transmitter caused a particular transition at the output.

When the preceeding analysis is performed for the case of three simultaneous transmissions, the results are not as successful. In this case, the object is to detect three zero crossings at the Format A Decoder output per sample period, T. However, in all cases, only two of the three expected zero crossings occur. Since the interceptor does not know which two transmitters cause the zero crossings that he does detect, he must guess according to some predetermined rule. Regardless of the rule, one third of the information has been lost and performance is degraded over the two transmission case.

Thus, for modulation format A, intercept and decoding of the message for the case of a single transmission is not possible without knowledge of the PN code used. However, as has been shown, for two simultaneous transmissions and under ideal conditions, the modulation format A waveform can be intercepted and decoded without knowledge of the PN codes used. As was pointed out, the fidelity of the reconstructed message will be degraded by additive noise, the phase offset between the transmitter carriers, and the offset between the code bits at the receiver. For three simultaneous transmissions, only partial decoding is possible since one third of the information is lost. In the next section, the Format B Decoder will be analyzed. It will be shown that decoding

a modulation format B waveform does not require more than one transmission as is true for the format A case.

Format B Decoder. Transmissions from generic transmitter model B, Figure 9, are processed by the Format B Decoder, shown in Figure 14. This configuration is a logical choice for the interceptor if he assumes the following:

1) The phase information is differentially encoded.

2) The rule used to map the voice samples to phase values is linear.

The second assumption is not ludicrous when one considers that for any continuous mapping rule, small variations around some operating point are nearly linear. In any case, the interceptor must assume some mapping rule, and a linear rule is as attractive as any. Based upon these assumptions, the interceptors estimate of the encoding rule is

$$\theta_k = (K_1 m_k + K_2) + \theta_{k-1} \tag{116}$$

where K_1 and K_2 are constants, m_k is the value of the sample on the k^{th} sample interval, and θ_k and θ_{k-1} are the encoded phase values for the k^{th} and $(k-1)^{st}$ samples. Thus, the interceptors decoding rule is the following:

$$m_k = \frac{1}{K_1} (\theta_k - \theta_{k-1}) - \frac{K_2}{K_1} \tag{117}$$

The interceptors first task, then, is to detect the phase values, θ_k and θ_{k-1}. Then, he must use his decoding rule, equation (117). These tasks are implemented by the hardware of Figure 14.

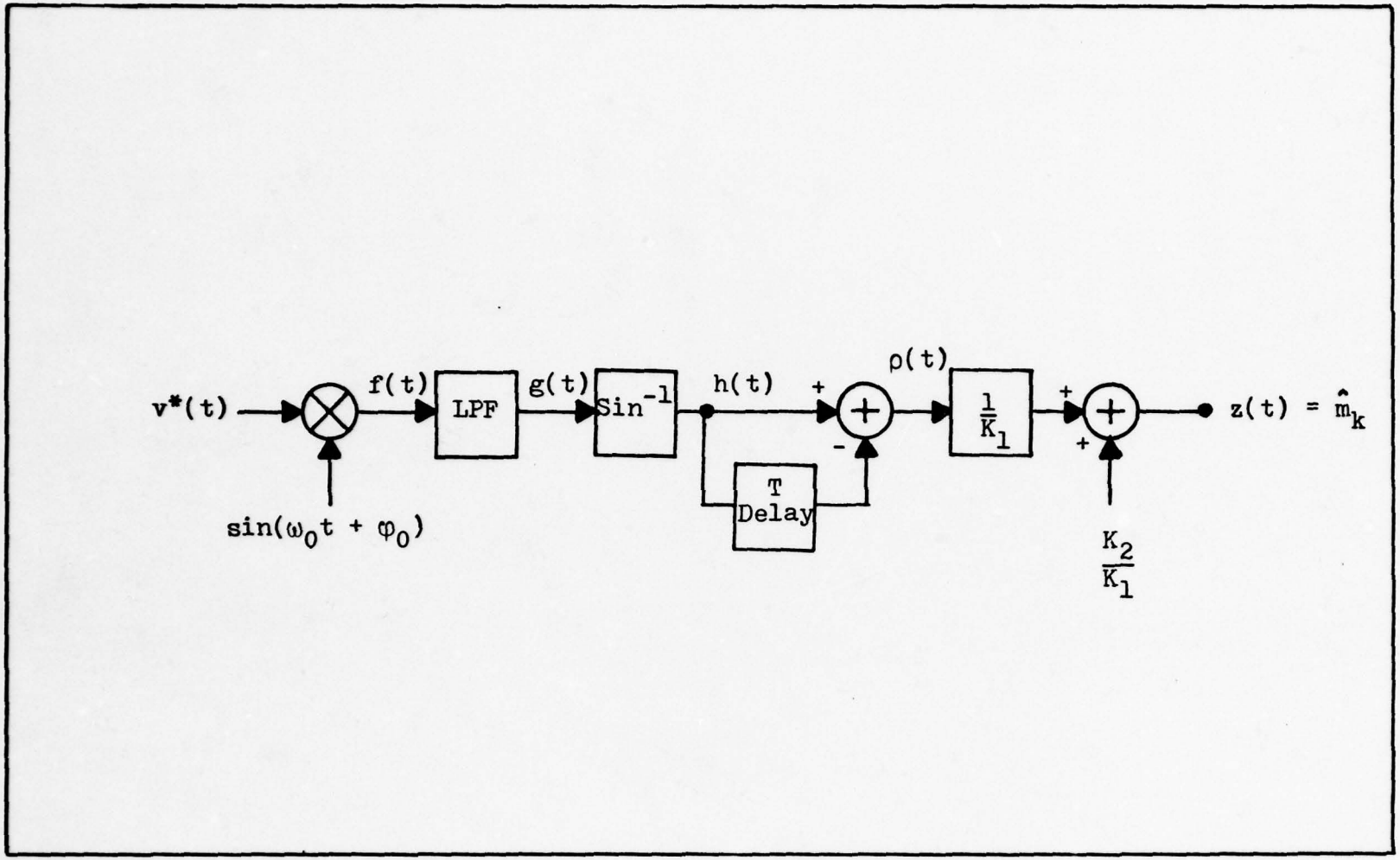


Figure 14. Format B Decoder

Assuming a negligible noise level, the input signal $v(t)$ is multiplied by a sinusoid at the carrier frequency to give

$$f(t) = -V \cos[\omega_0 t + \varphi(t)] \sin[\omega_0 t + \varphi_0]$$
$$= \frac{-V}{2} \sin[2\omega_0 t + \varphi(t) + \varphi_0] + \frac{V}{2} \sin[\varphi(t) - \varphi_0] \quad (118)$$

where φ_0 is a phase offset between the sinusoid and the input signal, and where $\varphi(t)$ is a phase term composed of encoded phase terms, $\theta(t)$, and some Doppler phase, $\theta_d(t)$, associated with the relative motion between the transmitter and intercept receiver. Thus

$$\varphi(t) = \theta(t) + \theta_d(t) \quad (119)$$

Equation (118) is filtered by a lowpass filter to give the following:

$$g(t) = \sin[\varphi(t) - \varphi_0] \quad (120)$$

This is processed to give

$$h(t) = \mathrm{Sin}^{-1}\{\sin[\varphi(t) - \varphi_0]\} = \varphi(t) - \varphi_0 \quad (121)$$

If it is assumed that the Doppler phase varies slowly enough so that it can be considered constant over a sampling interval and approximately equal from one interval to the next, then the following results occur. For the $(k-1)^{st}$ interval

$$h(t) = h_{k-1} = \hat{\theta}_{k-1} + \theta_d - \varphi_0 \quad (122)$$

For the k^{th} interval

$$h(t) = h_k = \hat{\theta}_k + \theta_d - \varphi_0 \tag{123}$$

Then

$$\rho(t) = h_k - h_{k-1} = \hat{\theta}_k - \hat{\theta}_{k-1} \tag{124}$$

The interceptor has now reconstructed the differential phase and will process it according to his decoding rule, equation (117). The output is then

$$\hat{m}_k = z(t) = \frac{1}{K_1} (\hat{\theta}_k - \hat{\theta}_{k-1}) - \frac{K_2}{K_1} \tag{125}$$

Recall that the transmitter used the following non-linear encoding rule:

$$\theta_k = 2 \cos^{-1}\left(\frac{1+m_k}{2}\right) + \theta_{k-1} \tag{126}$$

The function

$$\theta_k - \theta_{k-1} = 2 \cos^{-1}\left(\frac{1+m_k}{2}\right) \tag{127}$$

is graphed in Figure 15 over the range $-1 \leq m_k \leq 1$. Using equation (127) in (125), the sample estimate at the output becomes

$$\hat{m}_k = \frac{2}{K_1} \cos^{-1}\left(\frac{1+m_k}{2}\right) - \frac{K_2}{K_1} \tag{128}$$

As a measure of the accuracy of this estimate, it is useful to compute the Mean Square Error (MSE). This is defined as

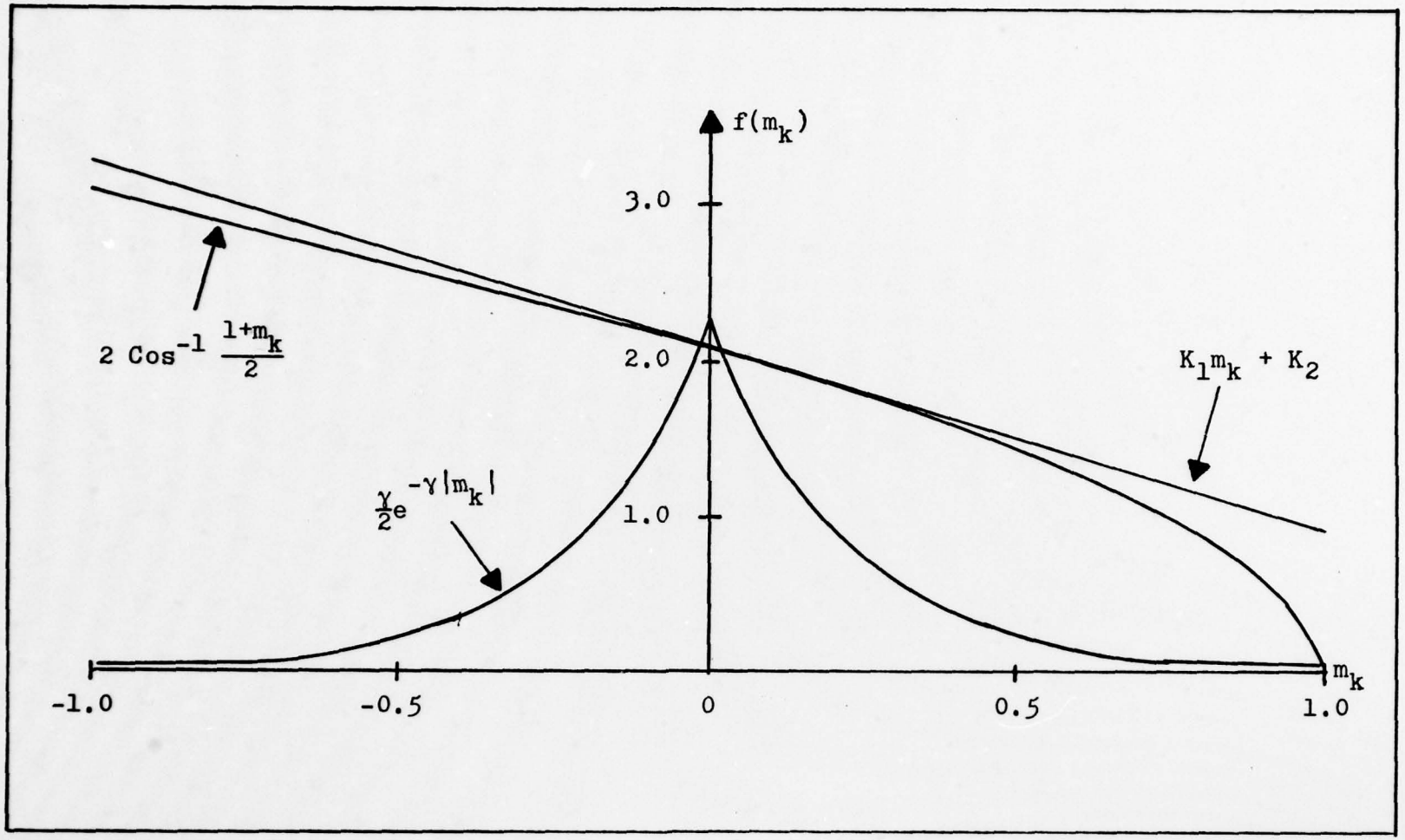


Figure 15. Format B Encoding Rule, PDF of Message Samples, and Interceptors Estimated Encoding Rule.

$$
\begin{aligned}
\text{MSE} &= E\{(m_k - \hat{m}_k)^2\} \\
&= E\{m_k^2\} - 2E\{m_k \hat{m}_k\} + E\{\hat{m}_k^2\} \\
&= E\{m_k^2\} - \frac{4}{K_1} E\left[m_k \cos^{-1}\left(\frac{1+m_k}{2}\right)\right] \\
&\quad + 2\frac{K_2}{K_1} E\{m\} + \frac{4}{K_1^2} E\left[\left[\cos^{-1}\left(\frac{1+m_k}{2}\right)\right]^2\right] \\
&\quad - 4\frac{K_2}{K_1^2} E\left[\cos^{-1}\left(\frac{1+m_k}{2}\right)\right] + E\left[\frac{K_2^2}{K_1^2}\right]
\end{aligned}
\tag{129}
$$

To evaluate the MSE further requires knowledge of the probability density function of m_k. Recall that the parameter m_k is an amplitude sample of a speech voltage waveform, m(t). An adequate model for a speech voltage waveform distribution is given by the Laplace distribution (Ref. 19:46). The associated probability density function is given by the following (Ref. 14):

$$
p(m) = \frac{\gamma}{2} \exp(-\gamma|m|) \qquad \gamma > 0 \tag{130}
$$

The parameter γ is determined as follows. Since the function $\cos^{-1}[(1+m_k)/2]$ is not defined for $|m_k|>1$, the original voice waveform was preprocessed such that the probability of m_k exceeding 1 would be very small. If m_k is arbitrarily constrained such that

$$
\Pr[|m_k|>1] \leq 0.01 \tag{131}
$$

then γ must be such that

$$
\int_{-1}^{1} \frac{\gamma}{2} \exp(-\gamma|m|)\, dm \geq 0.99 \tag{132}
$$

Solving this for γ gives

$$\gamma \geq - \ln(0.01) \approx 4.6052 \tag{133}$$

Using this value, the probability density function of m_k, also plotted in Figure 15, is given by the following:

$$p(m) = 2.3026 \exp(-4.6052|m|) \tag{134}$$

Its first and second moments are

$$E\{m_k\} = 0 \tag{135}$$

$$E\{m_k^2\} = \frac{2}{\gamma^2} = 0.0943 \tag{136}$$

Using this probability density function, the MSE, equation (129), can now be evaluated. The expectations involving $\text{Cos}^{-1}[(1+m_k)/2]$ were computed numerically to give the following equation for the MSE:

$$\begin{aligned} MSE = {} & 0.0943 + (0.20)/K_1 \\ & + (4.53 - 4.20K_2 + K_2^2)/K_1^2 \end{aligned} \tag{137}$$

The minimum MSE is found by taking the partial derivatives of the MSE with respect to K_1 and K_2, set them equal to zero, and solve simultaneously for K_1 and K_2. This procedure gives $K_1 = -1.2$ and $K_2 = 2.1$. The minimum MSE is now computed to be

$$MSE_{min} = 0.011 \tag{138}$$

The minimum MSE normalized to the a priori voice variance is

$$\frac{MSE_{min}}{E\{m_k^2\}} = 0.1163 \tag{139}$$

The interceptors linear decoding rule, equation (127), has also been plotted in Figure 15 using the values of K_1 and K_2 computed above. Notice how closely this approximates the actual non-linear rule used for small variations about zero. Thus, under the ideal conditions assumed, the output of the Format B Decoder closely approximates the transmitted message.

Unfortunately, ideal conditions are seldom encountered. The Doppler phase can cause significant errors. As a worst case example for a fixed intercept receiver, consider the case of the transmitter aboard an aircraft moving at Mach 2 relative to the receiver. Assume a transmitter frequency of f_0 = 250 MHz. The Doppler frequency, f_d, is (Ref. 13)

$$f_d = f_0(1-v/c) \tag{140}$$

where v is the aircraft velocity (662.72 m/sec) and c is the speed of light (2.998×10^8 m/sec). Thus, for the worst case

$$f_d = 249.9994474 \text{ MHz} \tag{141}$$

For a signal of the form $\cos[\omega_0 t + \theta_d(t)]$, the instantaneous phase is $\omega_0 t + \theta_d(t)$. The instantaneous angular frequency is

$$\omega = \frac{d}{dt}[\omega_0 t + \theta_d(t)] \tag{142}$$

Thus, the Doppler angular frequency, ω_d is:

$$\omega_d = 2\pi f_d = \omega_0 + \frac{d}{dt}[\theta_d(t)]$$

$$\omega_d = 2\pi f_0 + \frac{d}{dt}[\theta_d(t)] \tag{143}$$

Then, the Doppler phase is

$$\theta_d(t) = 2\pi \int_0^t (f_d - f_0)\, dt$$
$$= -2\pi(552.6)t \tag{144}$$

Suppose that the sampling rate is $f_s = 1/T = 8$ kHz. With $t = T$, the Doppler phase shift over one sample interval is

$$\theta_d(t) = -2\pi(552.6)T$$
$$= -0.43 \text{ radians/interval}$$
$$= -24.87 \text{ degrees/interval} \tag{145}$$

This is a significant error. Under most cases, the Doppler phase must be handled. If it is assumed that $\theta_d(t)$ changes at approximately a constant rate (corresponding to a constant aircraft velocity), then the following results occur. For the $(k-1)^{st}$ interval:

$$h_{k-1} = \hat{\theta}_{k-1} + \theta_d[(k-1)T + t] - \varphi_0 \tag{146}$$

For the k^{th} interval:

$$h_k = \hat{\theta}_k + \theta_d(kT + t) - \varphi_0 \tag{147}$$

Thus

$$\rho_k = h_k - h_{k-1} = (\hat{\theta}_k - \hat{\theta}_{k-1}) + \{\theta_d(kT+t) - \theta_d[(k-1)T+t]\} \tag{148}$$

and

$$z(t) = \frac{1}{K_1}(\hat{\theta}_k - \hat{\theta}_{k-1}) - \frac{K_2}{K_1} + \frac{1}{K_1}\{\theta_d(kT+t) - \theta_d[(k-1)T+t]\} \tag{149}$$

It is desired that the last term in equation (149) be zero to eliminate Doppler phase errors. One way to accomplish this is to estimate the Doppler phase and subtract it thru some type of decision directed feedback circuitry. This is also referred to as data aided feedback, decision feedback, modulation removal, or inverse modulation (Ref. 8:219-225 and 13:64). The interested reader is referred to these sources for a comprehensive look at this technique.

In this section, it was shown that the Format B Decoder can decode the intercepted signal if the additive noise is considered negligible, if the Doppler phase can be estimated, and if the rule used at the transmitter to map amplitude samples of the message into phase values is nearly linear, at least for small variations about zero. Unlike the case of modulation format A, decoding modulation format B does not require two simultaneous transmissions.

V Conclusions and Recommendations

Conclusions

This thesis has shown that for a class of modulation formats, intercept and message decoding of pseudo-noise encoded spread spectrum waveforms is possible without knowledge or duplication of the spreading code used, under appropriate conditions. The essential element necessary to accomplish this was processing of the received signals through non-linear elements (square law devices and fourth law devices). The non-linear devices had the effect of producing terms that had been stripped of code terms.

A general waveform equation was introduced as the primary tool in the analysis. This waveform equation could be adapted to fit a number of polyphase shift keyed modulation schemes. It was demonstrated that this general waveform equation encompassed O-QPSK, MSK, and SFSK modulation schemes when the appropriate pulse shaping function was used.

Two generic modulation formats, designated as format A and format B, and their associated transmitter models were introduced. It was shown that these formats fit the general waveform equation. In format A, the message was split into quadratures and encoded at baseband by two orthogonal PN codes prior to RF modulation. In format B, quadrature carriers were directly phase modulated with identical information prior to encoding by two orthogonal PN codes at RF.

An intercept receiver model was proposed. The general waveform equation was used as the input to the receiver and the receiver signals were computed. The receiver was divided into three main sections: the Carrier Reconstruction Loop; the Format A Decoder; and the Format B Decoder.

The Carrier Reconstruction Loop, composed of a quadrupling circuit and a PLL, was analyzed first. It was shown that regardless of the format used (A or B) or the pulse shaping used on the data (O-QPSK, MSK, or SFSK), there was a term produced at the output of the quadrupler that did not contain code terms. This term could be tracked by the PLL to produce coherent reference signals at the carrier frequency. In addition, for format B, this term contained the desired message information.

It was shown that for modulation format A, decoding the message without knowledge of the PN code was not possible for this receiver when only one transmission was received. It was demonstrated that when two simultaneous transmissions were received, message reconstruction of both transmissions was possible under the appropriate conditions. The output of the Format A Decoder was calculated for this case and the results showed that successful decoding depends upon the differences in the two transmitters carrier phases, the arrival offset between the PN code bits at the receiver, and additive noise. When ideal conditions were assumed (no carrier phase difference, no code offset, negligible noise) it was demonstrated that both transmitted messages could be reconstructed.

Under non-ideal conditions, the performance was degraded. For three simultaneous transmissions, one third of the desired information was not present at the output.

For modulation format B, decoding of the message was possible even when only one transmission was received. Factors which affected the success of decoding this format were additive noise, Doppler phase shift associated with the relative motion between the transmitter and receiver, and the extent to which the baseband modulation was linear.

Recommendations

The following recommendations for further study are made by the author. First, the signal to noise ratio of the quadrupling circuit output should be calculated for the case of MSK and SFSK modulation to verify the negligible noise power assumption made in Appendix A. Secondly, since the results in this thesis were developed for primarily ideal conditions, the analysis should be extended to quantify the conditions under which successful intercept and decoding is possible. It is also recommended that the signals and receiver performance be simulated on a computer to test the validity of the results of the extended analysis. If possible, hardware tests should be performed. Finally, it is recommended that other intercept methods be investigated, such as correlating a received signal with a delayed version of itself.

Bibliography

1. Amoroso, Frank. "Pulse and Spectrum Manipulation in the Minimum (Frequency) Shift Keying (MSK) Format," IEEE Transactions on Communications, COM-24 3: 381-384 (March 1976).

2. Bayless, Jon W. and Robert D. Pedersen. "Efficient Pulse Shaping Using MSK or PSK Modulation," IEEE Transactions on Communications, COM-27 6: 927-930 (June 1979).

3. Butman, Stanley A. and James R. Lesh. "The Effects of Bandpass Limiters on n-Phase Tracking Systems," IEEE Transactions on Communications, COM-25 6: 569-576 (June 1977).

4. Carlson, Bruce A. Communication Systems: An Introduction to Signals and Noise in Electrical Communication. New York: McGraw-Hill Book Company, 1968.

5. Craddock, Joseph L. "Analysis of Modern Digital Modulation Techniques," Air Force Institute of Technology, MS Thesis, AFIT/GE/EE/78-23, (December 1978).

6. Dixon, Robert C. Spread Spectrum Systems. New York: John Wiley and Sons, 1976.

7. -----, Ed. Spread Spectrum Techniques. New York: IEEE Press, 1976.

8. Gardner, Floyd M. Phaselock Techniques. New York: John Wiley and Sons, 1979.

9. Glazer, B. G. "Spread Spectrum Concepts," Proceedings of the 1973 Symposium on Spread Spectrum Communications, Naval Electronics Laboratory Center, San Diego, California, Vol. 1: 5-8 (March 1973).

10. Goulomb, Solomon W., Ed. Digital Communications with Space Applications. New Jersey: Prentice-Hall, Inc., 1964.

11. Gronemeyer, Stephen A. and Alan L. McBride. "MSK and Offset QPSK Modulation," IEEE Transactions on Communications, COM-24 8: 809-819 (August 1976).

12. Harris, R. L. "Introduction to Spread Spectrum Techniques," AGARD Lecture Series No. 58 on Spread Spectrum Communications, Bolkesjo, Norway, 3-1 to 3-21 (May 1973).

13. Lindsey, William C. and Marvin K. Simon. Telecommunications System Engineering. New Jersey: Prentice-Hall, Inc., 1973.

14. Papoulis, Athanasios. Probability, Random Variables, and Stochastic Processes. New York: McGraw-Hill Book Company, 1965.

15. Ristenbatt, Marlin P. "Pseudo-Random Binary Coded Waveforms," Modern Radar: Analysis, Evaluation, and System Design, R. S. Berkowitz, Ed. New York: John Wiley and Sons, 1965.

16. Ristenbatt, Marlin P. and James L. Daws, Jr. "Performance Criteria for Spread Spectrum Communications," IEEE Transactions on Communications, COM-25 8: 756-763 (August 1977).

17. Ristenbatt, Marlin P., James L. Daws, Jr. and H. M. Pearce. "Crack Resistant Sequences for Data Security," IEEE National Telecommunications Conference Record, Vol. 1: 15F1-15F5 (November 1973).

18. Simon, Marvin K. "A Generalization of Minimum-Shit-Keying (MSK)-Type Signaling Based Upon Input Data Symbol Pulse Shaping," IEEE Transactions on Communications, COM-24 8: 845-855 (August 1976).

19. Spilker, J. J., Jr. Digital Communications by Satellite. New Jersey: Prentice-Hall, Inc., 1977.

20. Van Trees, Harry L. Detection, Estimation, and Modulation Theory: Part I. New Jersey: Prentice-Hall, Inc., 1968.

21. Vertibi, A. J. Principles of Coherent Communication. New York: McGraw-Hill, 1966.

22. Ziemer, R. E. and W. H. Tranter. Principles of Communications: Systems, Modulation, and Noise. Boston: Houghton Mifflin Company, 1976.

Appendix A: Quadrupling Circuit Calculations

In this appendix, the output of the quadrupling circuit shown in Figure 16 will be calculated for input signals of the form of equation (48), repeated here.

$$r(t) = Aa_n p(t-nT_c) \cos[\omega_0 t + \varphi(t)] + Ab_n p(t-nT_c-T_c/2) \sin[\omega_0 t + \varphi(t)] + n(t) \quad (48)$$

The output equation developed here will be shown to be consistent with results in the open literature. The amplitudes of the signal components of the output, v(t), will be calculated for the cases of O-QPSK, MSK, and SFSK pulse shaping. Finally, the signal to noise ratio at the output will be calculated for O-QPSK pulse shaping.

The received signal is filtered to give

$$x(t) = [Aa_n p_a + n_c(t)] \cos[\omega_0 t + \varphi(t)] + [Ab_n p_b - n_s(t)] \sin[\omega_0 t + \varphi(t)] \quad (150)$$

In equation (150), p_a and p_b have been substituted for notational compactness for $p(t-nT_c)$ and $p(t-nT_c-T_c/2)$ respectively. Also, n(t) has been represented by its narrowband quadrature components, $n_c(t)$ and $n_s(t)$ (Ref. 22:237). Again, for notational compactness, the arguments of $n_c(t)$ and $n_s(t)$ will be dropped. Raising equation (150) to the fourth power and keeping only those terms in the vicinity of $4\omega_0$ gives the output of this circuit, v(t).

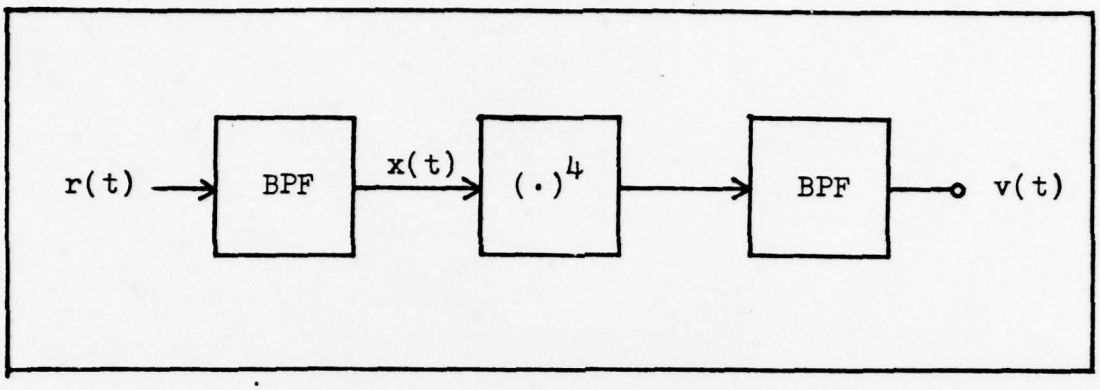


Figure 16. Quadrupling Circuit.

$$
\begin{aligned}
v(t) = {} & \left[\tfrac{1}{8}A^4p_a^4 + \tfrac{1}{8}A^4p_b^4 - \tfrac{3}{4}A^4p_a^2p_b^2\right]\cos[4\omega_0 t + 4\varphi(t)] \\
& + \left[\tfrac{1}{2}A^4a_nb_np_a^3p_b - \tfrac{1}{2}A^4a_nb_np_ap_b^3\right]\sin[4\omega_0 t + 4\varphi(t)] \\
& + \Big[\left(\tfrac{1}{2}A^3a_np_a^3 - \tfrac{3}{2}A^3a_np_ap_b^2\right)n_c + \left(\tfrac{3}{2}A^3b_np_a^2p_b - \tfrac{1}{2}A^3b_np_b^3\right)n_s \\
& + (3A^2a_nb_np_ap_b)n_cn_s + \left(-\tfrac{3}{2}Aa_np_a\right)n_cn_s^2 \\
& + \left(\tfrac{3}{2}Ab_np_b\right)n_c^2n_s + \left(\tfrac{3}{4}A^2p_a^2 - \tfrac{3}{4}A^2p_b^2\right)n_c^2 \\
& + \left(\tfrac{3}{4}A^2p_b^2 - \tfrac{3}{4}A^2p_a^2\right)n_s^2 - \tfrac{3}{4}n_c^2n_s^2 + \left(\tfrac{1}{2}Aa_np_a\right)n_c^3 \\
& + \left(-\tfrac{1}{2}Ab_np_b\right)n_s^3 + \tfrac{1}{8}n_c^4 + \tfrac{1}{8}n_s^4\Big]\cos[4\omega_0 t + 4\varphi(t)] \\
& + \Big[\left(\tfrac{3}{2}A^3b_np_a^2p_b - \tfrac{A^3}{2}b_np_b^3\right)n_c + \left(\tfrac{3}{2}A^3a_np_ap_b^2 - \tfrac{1}{2}A^3a_np_a^3\right)n_s \\
& + \left(\tfrac{3}{2}A^2p_b^2 - \tfrac{3}{2}A^2p_a^2\right)n_cn_s + \left(-\tfrac{3}{2}Ab_np_b\right)n_cn_s^2 \\
& + \left(-\tfrac{3}{2}Aa_np_a\right)n_c^2n_s + \left(\tfrac{3}{2}A^2a_nb_np_ap_b\right)n_c^2 \\
& + \left(-\tfrac{3}{2}A^2a_nb_np_ap_b\right)n_s^2 + \left(\tfrac{1}{2}Ab_np_b\right)n_c^3 + \left(\tfrac{1}{2}Aa_np_a\right)n_s^3 \\
& + \tfrac{1}{2}n_cn_s^3 - \tfrac{1}{2}n_c^3n_s\Big]\sin[4\omega_0 t + 4\varphi(t)] \qquad (151)
\end{aligned}
$$

It would be nice to compare this equation with a known result for verification. To do this, consider the case of O-QPSK (rectangular) pulse shaping and no PN coding. In the equation, this corresponds to letting $a_n = b_n = 1$, and $p_a = p_b = 1$. With $\varphi(t) = 0$, the output of the quadrupling circuit is then:

$$\begin{aligned} v(t) = & -\tfrac{1}{2}A^4 \cos(4\omega_0 t) \\ & + \Big[-A^3 n_c + A^3 n_s + 3A^2 n_c n_s - \tfrac{3}{2}A n_c n_s^2 \\ & + \tfrac{3}{2}A n_c^2 n_s - \tfrac{3}{4}n_c^2 n_s^2 + \tfrac{1}{2}A n_c^3 - \tfrac{1}{2}A n_s^3 \\ & + \tfrac{1}{8}n_c^4 + \tfrac{1}{8}n_s^4\Big] \cos(4\omega_0 t) \\ & + \Big[A^3 n_c + A^3 n_s - \tfrac{3}{2}A n_c n_s^2 - \tfrac{3}{2}A n_c^2 n_s \\ & + \tfrac{3}{2}A^2 n_c^2 - \tfrac{3}{2}A^2 n_s^2 + \tfrac{1}{2}A n_c^3 + \tfrac{1}{2}A n_s^3 \\ & + \tfrac{1}{2}n_c n_s^3 - \tfrac{1}{2}n_c^3 n_s\Big] \sin(4\omega_0 t) \end{aligned} \tag{152}$$

An identical result is obtained by Butman and Lesh (Ref. 3). The input signal in their article is

$$r(t)' = s(t)' + n(t)' \tag{153}$$

where $n(t)'$ is zero mean, white, Gaussian noise and

$$s(t)' = \sqrt{2}A \cos(\omega_0 t + 2i\pi/4) \qquad i = 0,1,2,3 \tag{154}$$

Notice that $s(t)'$ can take on any one of four values designated s_0', s_1', s_2', and s_3'. Figure (17) is the signal space representation of $r(t)'$ in the r_1', r_2' plane. In the figure, $n(t)'$ is shown in its quadrature component representation,

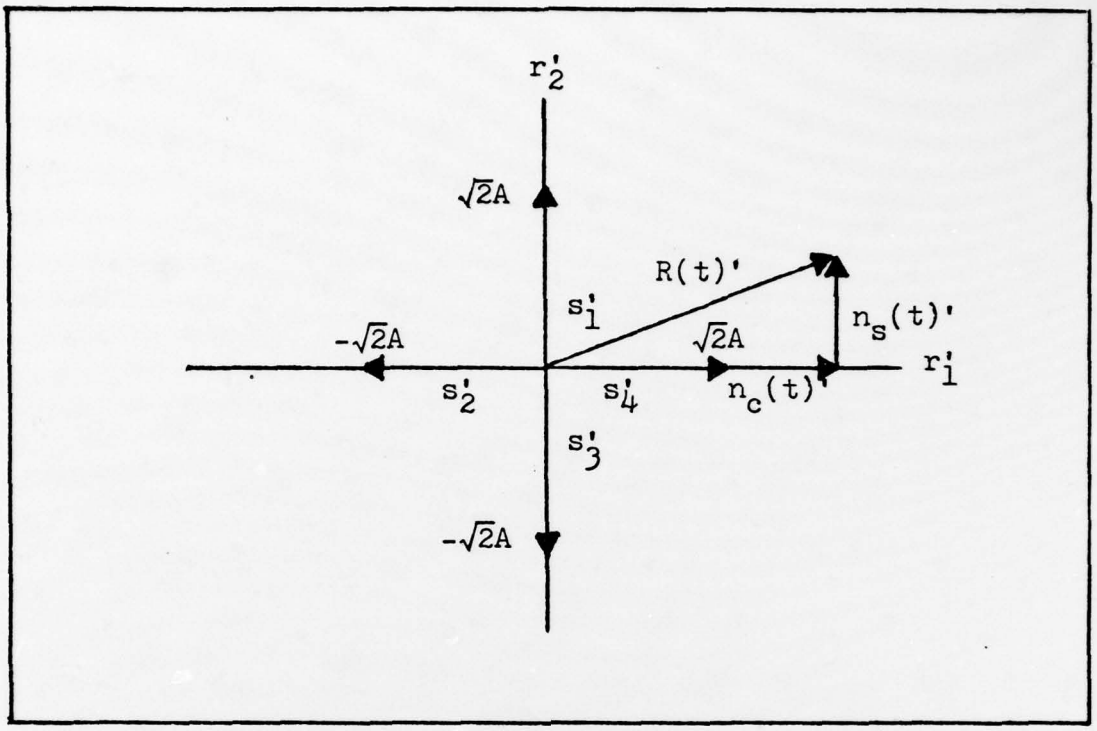


Figure 17. Signal Space Representation of the Received Signal, r(t)'.

$n_c(t)'$ and $n_s(t)'$. The filtered signal is given as

$$r*(t)' = R(t)' \cos[\omega_0 t + 2i\pi/4 + \Phi(t)] \qquad (155)$$

where

$$R(t)' = \{[\sqrt{2}A + n_c(t)']^2 + n_s^2(t)'\}^{\frac{1}{2}} \qquad (156)$$

and

$$\Phi(t)' = \mathrm{Tan}^{-1}\{n_s(t)'/[\sqrt{2}A + n_c(t)']\} \qquad (157)$$

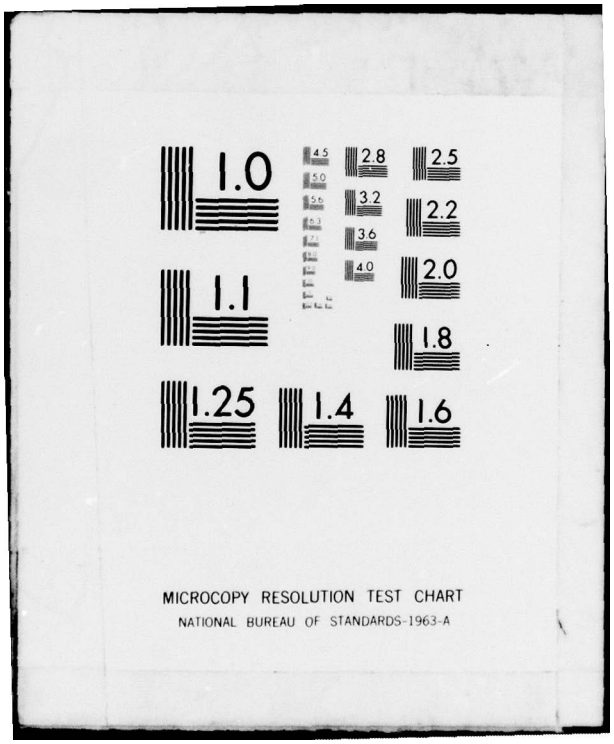
Raising this to the 4^{th} power and retaining only terms around $4\omega_0$ gives the output,

$$v(t)' = \frac{R^4(t)'}{8} \cos[4\omega_0 t + 4\Phi(t)] \qquad (158)$$

AD-A080 213 AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOO--ETC F/G 17/4
INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED--ETC(U)
DEC 79 T J HALL
UNCLASSIFIED AFIT/GE/EE/79-15 NL

2 OF 2
AD
A080213

END
DATE
FILMED
3-80
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Using equations (156), (157), several trigonometric identities, and dropping the arguments of $n_c(t)'$ and $n_s(t)'$, equation (158) becomes the following:

$$
\begin{aligned}
v(t)' = {} & \tfrac{1}{2}A^4 \cos(4\omega_0 t) \\
& + \left[\sqrt{2}A^3 n_c' - \tfrac{3}{2}A^2 n_c^2{}' + \tfrac{3}{2}A^2 n_s^2{}' - \tfrac{3}{2}\sqrt{2}A n_c' n_s^2{}' \right. \\
& \left. + \tfrac{3}{4}n_c^2{}' n_s^2{}' + \tfrac{\sqrt{2}}{2}A n_c^3{}' + \tfrac{1}{8}n_c^4{}' + \tfrac{1}{8}n_s^4{}' \right] \cos(4\omega_0 t) \\
& + \left[-\sqrt{2}A^3 n_s' + 3A^2 n_c' n_s' - \tfrac{3\sqrt{2}}{2}A n_c^2{}' n_s' \right. \\
& \left. + \tfrac{\sqrt{2}}{2}A n_s^3{}' - \tfrac{1}{2}n_c' n_s^3{}' + \tfrac{1}{2}n_c^3{}' n_s' \right] \sin(4\omega_0 t) \qquad (159)
\end{aligned}
$$

Equations (152) and (159) do not appear to be identical until the differences in the signal representation are taken into account. For the example at hand, equation (48) can be written equivalently as

$$
\begin{aligned}
r(t) &= s(t) + n(t) \\
&= \sqrt{2}A \cos[\omega_0 t + (2i+1)\pi/4] \\
&\quad + n(t) \qquad i = 0,1,2,3 \qquad (160)
\end{aligned}
$$

Figure 18 shows the corresponding signal space representation for this case. From Figure 17 and 18, it is clear that

$$n_c(t)' = \tfrac{\sqrt{2}}{2}n_c(t) - \tfrac{\sqrt{2}}{2}n_s(t) \qquad (161)$$

and

$$n_s(t)' = \tfrac{\sqrt{2}}{2}n_c(t) + \tfrac{\sqrt{2}}{2}n_s(t) \qquad (162)$$

When the differences in the signal and noise representations are taken into account, equation (159) can be shown to be equivalent to (152). Thus, equation (151) appears correct.

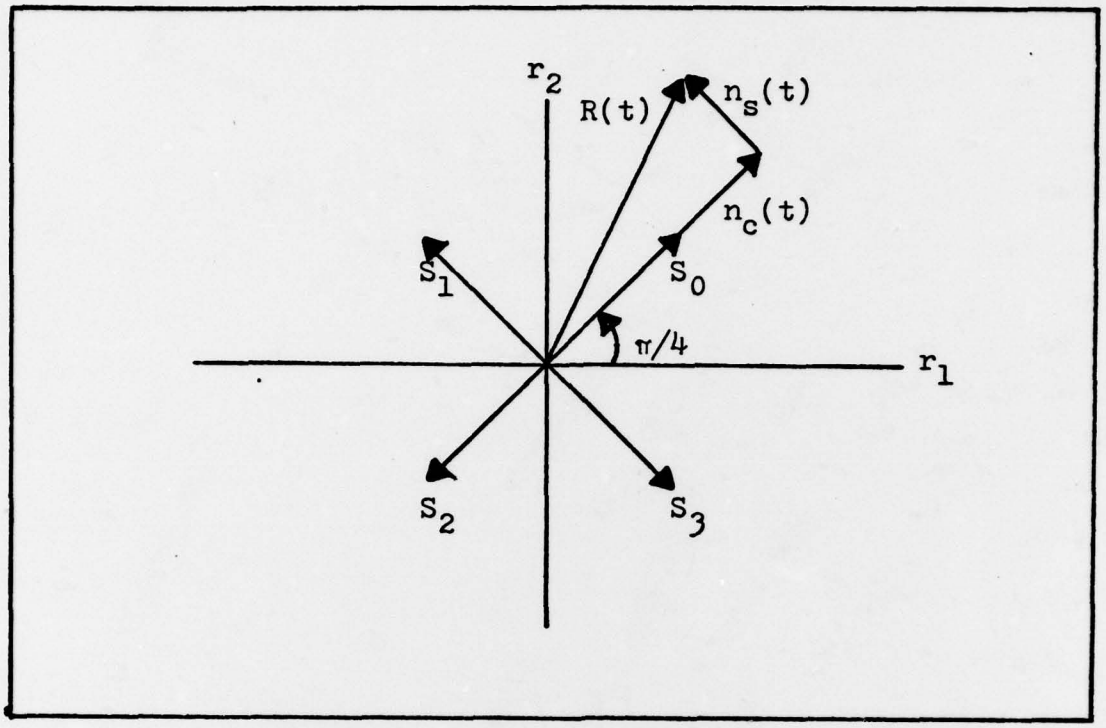


Figure 18. Signal Space Representation of the Received Signal, r(t).

The output, equation (151), is now rewritten as

$$v(t) = \left[\frac{1}{8}A^4p_a^4 + \frac{1}{8}A^4p_b^4 - \frac{3}{4}A^4p_a^2p_b^2\right]\cos[4\omega_0 t + 4\varphi(t)]$$

$$+\left[\frac{1}{2}A^4a_n b_n p_a^3 p_b - \frac{1}{2}A^4a_n b_n p_a p_b^3\right]\sin[4\omega_0 t + 4\varphi(t)]$$

$$+ N_c(t)\cos[4\omega_0 t + 4\varphi(t)]$$

$$+ N_s(t)\sin[4\omega_0 t + 4\varphi(t)] \qquad (163)$$

where $N_c(t)$ and $N_s(t)$ are noise terms whose definitions are apparent from a comparison of equations (151) and (163). The "signal" terms will be defined to be the first two expressions, and the noise terms the last two expressions

of equation (163). The signal terms will now be evaluated for the cases of O-QPSK, MSK, and SFSK pulse shaping.

The pulse shaping function for O-QPSK is given by equation (33). From this, it is clear that

$$p^m(t-nT_c) = \begin{cases} 1 & nT_c - T_c/2 < t < nT_c + T_c/2 \\ 0 & \text{elsewhere} \end{cases} \quad (164)$$

and

$$p^m(t-nT_c-T_c/2) = \begin{cases} 1 & nT_c < t < (n+1)T_c \\ 0 & \text{elsewhere} \end{cases} \quad (165)$$

These expressions are substituted into equation (163). The signal component becomes the following:

$$S_{O\text{-}QPSK} = \frac{-A}{2}^4 \cos[4\omega_0 t + 4\varphi(t)] \quad (166)$$

The average power in this signal is:

$$P_s = \frac{1}{T}\int_0^T \frac{-A}{2}^4 \cos[\omega_0 t + 4\varphi(t)]^2 dt$$

$$= \frac{A}{8}^8 = 0.1250\ A^8 \quad (167)$$

From equation (34), the following is true for MSK modulation:

$$p^m(t-nT_c) = (-1)^{nm} \cos^m(\pi t/T_c)$$

$$\text{for } nT_c - T_c/2 < t < nT_c + T_c/2$$

$$= 0 \qquad \text{elsewhere} \quad (168)$$

$$p^m(t-nT_c-T_c/2) = (-1)^{nm}\sin^m(\pi t/T_c)$$

$$\text{for } nT_c < t < (n+1)T_c$$

$$= 0 \qquad \text{elsewhere} \qquad (169)$$

These are substituted into the signal terms of equation (163) to give:

$$S_{MSK} = \left[\frac{A}{8}^4 \cos^4\left(\frac{\pi t}{T_c}\right) + \frac{A}{8}^4 \sin^4\left(\frac{\pi t}{T_c}\right) - 3A^4 \cos^2\left(\frac{\pi t}{T_c}\right)\sin^2\left(\frac{\pi t}{T_c}\right)\right]$$

$$\cdot \cos[4\ _0t + 4\ (t)]$$

$$+ \left[\frac{A}{8}^4 a_n b_n \cos^3\left(\frac{\pi t}{T_c}\right)\sin\left(\frac{\pi t}{T_c}\right) - \frac{A}{8}^4 a_n b_n \sin^3\left(\frac{\pi t}{T_c}\right)\cos\left(\frac{\pi t}{T_c}\right)\right]$$

$$\cdot \sin[4\omega_0 t + 4\varphi(t)]$$

$$= \frac{3A}{64}^4 \cos[4\omega_0 t + 4\varphi(t)]$$

$$+ \left[\frac{5A^4}{128} - \frac{2A^4}{128}a_n b_n\right] \cos\left[4\omega_0 t + 4\varphi(t) + \frac{4\pi t}{T_c}\right]$$

$$+ \left[\frac{5A^4}{128} + \frac{2A^4}{128}a_n b_n\right] \sin\left[4\omega_0 t + 4\varphi(t) - \frac{4\pi t}{T_c}\right] \qquad (170)$$

Since the first term in this equation is the only one near $4\omega_0$, it is the only one that actually appears in the output of the quadrupling circuit. The last two terms would be filtered. Thus, the signal output for MSK modulation is

$$S_{MSK} = \frac{3A}{64}^4 \cos[4\omega_0 t + 4\varphi(t)] \qquad (171)$$

and its average power is

$$P_s = \frac{9A^8}{8192} = 0.0011\ A^8 \qquad (172)$$

A similar treatment can be given for SFSK modulation. Using equation (35), the following equations result:

$$p^m(t-nT_c) = (-1)^{nm} \cos^m\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right]$$

$$\text{for } (nT_c - T_c/2) < t < (nT_c + T_c/2)$$

$$= 0 \qquad \text{elsewhere} \qquad (173)$$

$$p^m(t-nT_c-T_c/2) = (-1)^{nm} \sin^m\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right]$$

$$\text{for } nT_c < t < (n+1)T_c$$

$$= 0 \qquad \text{elsewhere} \qquad (174)$$

Substituting these expressions into equation (163) and letting $q = \frac{1}{4}\sin\left(\frac{4\pi t}{T_c}\right)$ the signal term for SFSK modulation is:

$$S_{SFSK} = \left[\frac{A^4}{8}\cos^4\left(\frac{\pi t}{T_c} - q\right) + \frac{A^4}{8}\sin^4\left(\frac{\pi t}{T_c} - q\right)\right.$$

$$\left. - \frac{3A^4}{8}\cos^2\left(\frac{\pi t}{T_c} - q\right)\sin^2\left(\frac{\pi t}{T_c} - q\right)\right]\cos[4\omega_0 t + 4\varphi(t)]$$

$$+ \left[\frac{A^4}{8}a_n b_n \cos^3\left(\frac{\pi t}{T_c} - q\right)\sin\left(\frac{\pi t}{T_c} - q\right)\right.$$

$$\left. - \frac{A^4}{8}a_n b_n \cos\left(\frac{\pi t}{T_c}\right)\sin^3\left(\frac{\pi t}{T_c} - q\right)\right]\sin[4\omega_0 t + 4\varphi(t)] \qquad (175)$$

Using trigonometric substitutions, rearranging terms, and substituting for q gives

$$S_{SFSK} = \frac{3A^4}{64} \cos[4\omega_0 t + 4\varphi(t)]$$

$$+ \left[\frac{5A^4}{128} - \frac{2A^4}{128} a_n b_n\right] \cos\left[4\omega_0 t + 4\varphi(t) + \frac{4\pi t}{T_c} - \sin \frac{4\pi t}{T_c}\right]$$

$$+ \left[\frac{5A^4}{128} + \frac{2A^4}{128} a_n b_n\right] \cos\left[4\omega_0 t + 4\varphi(t) - \frac{4\pi t}{T_c} + \sin \frac{4\pi t}{T_c}\right] \quad (176)$$

Letting $\omega_c = 2\pi/T_c = 2\pi f_c$, this becomes

$$S = \frac{3A^4}{64} \cos[4\omega_0 t + 4\varphi(t)]$$

$$+ \left[\frac{5A^4}{128} - \frac{2A^4}{128} a_n b_n\right] \cos[4\omega_0 t + 4\varphi(t) + 2\omega_c t - \sin(2\omega_c t)]$$

$$+ \left[\frac{5A^4}{128} + \frac{2A^4}{128} a_n b_n\right] \sin[4\omega_0 t + 4\varphi(t) - 2\omega_c t + \sin(2\omega_c t)] \quad (177)$$

To evaluate this further, let

$$\omega_s = 4\omega_0 + 2\omega_c \quad (178)$$

$$\omega_d = 4\omega_0 - 2\omega_c \quad (179)$$

$$\omega_m = 2\omega_c \quad (180)$$

Then

$$S_{SFSK} = \frac{3A^4}{64} \cos[4\omega_0 t + 4\varphi(t)]$$

$$+ \left[\frac{5A^4}{128} - \frac{2A^4}{128} a_n b_n\right] \cos[\omega_s t + 4\varphi(t) - \sin(\omega_m t)]$$

$$+ \left[\frac{5A^4}{128} + \frac{2A^4}{128} a_n b_n\right] \cos[\omega_d t + 4\varphi(t) + \sin(\omega_m t)] \quad (181)$$

Since

$$\cos[\omega t + \nu + \mu \sin(\omega_m t)] = \sum_n J_n(\mu) \cos[(\omega + n\omega_m)t + \nu] \quad (182)$$

then equation (181) becomes (with all substitutions removed):

$$\begin{aligned} S_{SFSK} &= \frac{3A^4}{64} \cos[4\omega_0 t + 4\varphi(t)] \\ &+ \left[\frac{5A^4}{128} - \frac{2A^4}{128} a_n b_n\right] \sum_n J_n(1) \cos\left[4\omega_0 t - (n-1)\frac{4\pi t}{T_c} + 4\varphi(t)\right] \\ &+ \left[\frac{5A^4}{128} + \frac{2A^4}{128} a_n b_n\right] \sum_n J_n(1) \cos\left[4\omega_0 t + (n-1)\frac{4\pi t}{T_c} + 4\varphi(t)\right] \end{aligned} \quad (183)$$

From a table of Bessel functions it is clear that the only significant terms in the summations involve $J_{-2}(1)$, $J_{-1}(1)$, $J_0(1)$, $J_1(1)$ and $J_2(1)$. For n equal to -2, -1, 0, or 2, the term is outside the bandwidth of the final filter. Then the signal output for SFSK modulation is:

$$\begin{aligned} S_{SFSK} &= \frac{3A^4}{64} \cos[4\omega_0 t + 4\varphi(t)] \\ &+ \left[\frac{5A^4}{128} - \frac{2A^4}{128} a_n b_n\right] J_1(1) \cos[4\omega_0 t + 4\varphi(t)] \\ &+ \left[\frac{5A^4}{128} + \frac{2A^4}{128} a_n b_n\right] J_1(1) \cos[4\omega_0 t + 4\varphi(t)] \\ &= \left[\frac{3A^4}{64} + \frac{5A^4}{64} \cdot J_1(1)\right] \cos[4\omega_0 t + 4\varphi(t)] \end{aligned} \quad (184)$$

The average power of this signal is given by

$$P_s = 0.0033\ A^8 \quad (185)$$

The output signals and their average power have been listed in Table III for comparison. Note the significant

reduction in the average power at the output for MSK and SFSK compared to O-QPSK. MSK shows a decrease of 20.56 dB from O-QPSK modulation and SFSK has a decrease of 15.78 dB from the O-QPSK signal. It can be argued heuristically that the noise power suffers a comparable loss since the noise terms are subject to the pulse shaping functions also, but this remains to be proven.

The signal to noise ratio (SNR) at the output of the quadrupling circuit will now be calculated for the case of O-QPSK pulse shaping, and an example will be given with reasonable numbers assigned. In this case, the noise output of the quadrupler reduces to the following:

$$
\begin{aligned}
N_{O\text{-}QPSK} = \Big[& -A^3 a_n n_c + A^3 b_n n_s + 3A^2 a_n b_n n_c n_s - \tfrac{3}{2} A a_n n_c n_s^2 \\
& + \tfrac{3}{2} A b_n n_c^2 n_s - \tfrac{3}{4} n_c^2 n_s^2 + \tfrac{1}{2} A a_n n_c^3 - \tfrac{1}{2} A b_n n_s^3 \\
& + \tfrac{1}{8} n_c^4 + \tfrac{1}{8} n_s^4 \Big] \cos[4\omega_c t + 4\varphi(t)] \\
& + A^3 b_n n_c + A^3 a_n n_s - \tfrac{3}{2} A b_n n_c n_s^2 - \tfrac{3}{2} A a_n n_c^2 n_s \\
& + \tfrac{3}{2} A^2 a_n b_n n_c^2 - \tfrac{3}{2} A^2 a_n b_n n_s^2 + \tfrac{1}{2} A b_n n_c^3 + \tfrac{1}{2} A a_n n_s^3 \\
& + \tfrac{1}{2} n_c n_s^3 - \tfrac{1}{2} n_c^3 n_s \sin[4\omega_c t + 4\varphi(t)] \qquad (186)
\end{aligned}
$$

The noise power is found by squaring this and taking the expected value with respect to the statistics of n_c and n_s. To evaluate this expected value, equation (52) was used with W equal to the noise bandwidth, and the following relation was used (Ref. 14:147):

TABLE III

Quadrupling Circuit Output Signal and Average Power.

Modulation Type	Output Signal	Average Power
O-QPSK	$-\frac{A}{2}^4 \cos[4\omega_0 t + 4\varphi(t)]$	$0.1250\ A^8$
MSK	$\frac{3A}{64}^4 \cos[4\omega_0 t + 4\varphi(t)]$	$0.0011\ A^8$
SFSK	$\left[\frac{3A}{64}^4 + \frac{5A}{64}^4 J_1(1)\right] \cos[4\omega_0 t + 4\varphi(t)]$	$0.0033\ A^8$

$$E\{n^m(t)\} = \begin{cases} 1\cdot 3\cdots(m-1)(N_0W)^{m/2} & m \text{ even} \\ 0 & m \text{ odd} \end{cases} \quad (187)$$

In addition, it was assumed that a_n, b_n, $n_c(t)$, and $n_s(t)$ were mutually independent of each other and zero mean. Performing the operations gives the following as the noise power output:

$$P_N = \frac{256\ A^6(N_0W) + 720\ A^4(N_0W)^2 + 448\ A^2(N_0W)^3 + 43(N_0W)^4}{128} \quad (188)$$

The signal to noise power ratio for the case of O-QPSK modulation is given by

$$\left(\frac{S}{N}\right)_{O\text{-}QPSK} = \frac{16\ A^8}{256\ A^6N_0W + 720\ A^4(N_0W)^2 + 448\ A^2(N_0W)^3 + 43(N_0W)^4} \quad (189)$$

Suppose the intercept receiver is located 10 miles from the transmitter whose effective radiated power is 100 watts and that the transmission frequency is 250 MHz. The received signal power is given by (Ref. 13:12)

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \tag{190}$$

where P_r is the received power; P_t is the transmitted power; G_t and G_r are the transmitter and receiver antenna gains, both assumed equal to 1 in this example; λ is the wavelength, and d is the distance between transmitter and receiver. Then the received signal power is

$$P_r = 3.5208295 \times 10^{-9} \text{ watts} = -54.53 \text{ dBm} \tag{191}$$

Since the signal power at the input is A^2, then

$$A = 5.9337 \times 10^{-5} \text{ volts} \tag{192}$$

The noise power bandwidth, W, is 16 KHz in this example and (Ref. 13:13)

$$N_0 = kT^\circ \tag{193}$$

where k represents Boltzmans constant (1.38×10^{-23} w/Hz-°K) and T° is the receiver noise temperature in degrees Kelvin (°K). If this is assumed to be room temperature (290°K), then

$$N_0 W = 6.4032 \times 10^{-17} \text{ watts} \tag{194}$$

Then the quadrupling circuit output SNR is, for this example:

$$\left(\frac{S}{N}\right)_{O\text{-QPSK}} = 3.437 \times 10^6 = 65.36 \text{ dB} \tag{195}$$

Thus, for this example, the SNR is quite large. If the noise power output for the case of MSK and SFSK modulation is equivalent to the O-QPSK case, then their SNR's would be on the order of 45 dB and 50 dB respectively, both of which are still large and more than adequate for the purposes of this thesis.

Appendix B: Format A Decoder Calculations for Two Transmissions

In this appendix, the outputs of the Format A Decoder, shown in Figure 12, will be calculated for the case where two simultaneous transmissions are received. The results will be evaluated for O-QPSK, MSK, and SFSK modulation.

The input signal, x(t), to the Format A Decoder is given by equation (79). After mixing with coherent carriers and filtering, the signals are:

$$x_I^*(t) = \tfrac{1}{2}A_1 a_{n1} p(t-nT_c) + \tfrac{\alpha}{2}A_2 a_{n2} p(t-nT_c-\Delta t) + \tfrac{\beta}{2}A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t) + \tfrac{1}{2}n_c(t) \quad (196)$$

$$x_Q^*(t) = \tfrac{1}{2}A_1 b_n p(t-nT_c-T_c/2) + \tfrac{\alpha}{2}A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t) - \tfrac{\beta}{2}A_2 a_{n2} p(t-nT_c-\Delta t) - \tfrac{1}{2}n_s(t) \quad (197)$$

The signals are processed thru the square law devices to give

$$u_I(t) = \tfrac{1}{4}A_1^2 p^2(t-nT_c) + \tfrac{\alpha^2}{4}A_2^2 p^2(t-nT_c-\Delta t) + \tfrac{\beta^2}{4}A_2^2 p^2(t-nT_c-T_c/2-\Delta t) + \tfrac{\alpha}{2}A_1 A_2 a_{n1} a_{n2} p(t-nT_c)\, p(t-nT_c-\Delta t) + \tfrac{\beta}{2}A_1 A_2 a_{n1} b_{n2} p(t-nT_c)\, p(t-nT_c-T_c/2-\Delta t) + \tfrac{\alpha\beta}{2}A_2^2 a_{n2} b_{n2} p(t-nT_c-\Delta t)\, p(t-nT_c-T_c/2-\Delta t)$$

$$+ \left[\frac{1}{2}A_1 a_{n1} p(t-nT_c) + \frac{\alpha}{2}A_2 a_{n2} p(t-nT_c-\Delta t) + \frac{\beta}{2}A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t)\right] n_c(t) + \frac{1}{4}n_c^2(t) \qquad (198)$$

and

$$\begin{aligned} u_Q(t) = {} & \frac{1}{4}A_1^2 p^2(t-nT_c-T_c/2) + \frac{\alpha^2}{4}A_2^2 p^2(t-nT_c-T_c/2-\Delta t) \\ & + \frac{\beta^2}{4}A_2^2 p^2(t-nT_c-\Delta t) \\ & + \frac{\alpha}{2}A_1 A_2 b_{n1} b_{n2} p(t-nT_c-T_c/2)\, p(t-nT_c-T_c/2-\Delta t) \\ & - \frac{\beta}{2}A_1 A_2 a_{n2} b_{n1} p(t-nT_c-\Delta t)\, p(t-nT_c-T_c/2) \\ & - \frac{\alpha\beta}{2}A_2^2 a_{n2} b_{n2} p(t-nT_c-\Delta t)\, p(t-nT_c-T_c/2-\Delta t) \\ & - \left[\frac{1}{2}A_1 b_{n1} p(t-nT_c-T_c/2) + \frac{\alpha}{2}A_2 b_{n2} p(t-nT_c-T_c/2-\Delta t) \right. \\ & \left. - \frac{\beta}{2}A_2 a_{n2} p(t-nT_c-\Delta t)\right] n_s(t) + \frac{1}{4}n_s^2(t) \end{aligned} \qquad (199)$$

For O-QPSK modulation, this becomes

$$\begin{aligned} u_I(t) = {} & \frac{1}{4}A_1^2 + \frac{1}{4}A_2^2(\alpha^2+\beta^2) \\ & + \frac{\alpha}{2}A_1 A_2 a_{n1} a_{n2} + \frac{\beta}{2}A_1 A_2 a_{n1} b_{n2} \\ & + \frac{\alpha\beta}{2}A_2^2 a_{n2} b_{n2} \\ & + \left[\frac{1}{2}A_1 a_{n1} + \frac{\alpha}{2}A_2 a_{n2} + \frac{\beta}{2}A_2 a_{n2}\right] n_c(t) + \frac{1}{4}n_c^2(t) \end{aligned} \qquad (200)$$

and

$$u_Q(t) = \frac{1}{4}A_1^2 + \frac{1}{4}A_2^2(\alpha^2+\beta^2)$$

$$+ \frac{\alpha}{2}A_1A_2b_{n1}b_{n2} - \frac{\beta}{2}A_1A_2a_{n2}b_{n1}$$

$$- \frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}$$

$$- \left[\frac{1}{2}A_1b_{n1} + \frac{\alpha}{2}A_2b_{n2} - \frac{\beta}{2}A_2a_{n2}\right]n_s(t) + \frac{1}{4}n_s^2(t) \qquad (201)$$

The outputs are then

$$y_I(t) = \frac{\alpha}{2}A_1A_2a_{n1}a_{n2} + \left[\frac{\beta}{2}A_1A_2a_{n1}b_{n2}\right]_{LP}$$
$$+ \left[\frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\right]_{LP} + \left[\frac{1}{4}n_c^2(t)\right]_{LP}$$
$$+ \left[\left(\frac{1}{2}A_1a_{n1} + \frac{\alpha}{2}A_2a_{n2} + \frac{\beta}{2}A_2a_{n2}\right)n_c(t)\right]_{LP} \qquad (202)$$

and

$$y_Q(t) = \frac{\alpha}{2}A_1A_2b_{n1}b_{n2} - \left[\frac{\beta}{2}A_1A_2a_{n2}b_{n1}\right]_{LP}$$
$$- \left[\frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\right]_{LP} + \left[\frac{1}{4}n_s^2(t)\right]_{LP}$$
$$- \left[\left(\frac{1}{2}A_1b_{n1} + \frac{\alpha}{2}A_2b_{n2} - \frac{\beta}{2}A_2a_{n2}\right)n_s(t)\right]_{LP} \qquad (203)$$

For MSK modulation

$$u_I(t) = \frac{1}{4}A_1^2\cos^2\left(\frac{\pi t}{T_c}\right) + \frac{\alpha^2}{4}A_2^2\cos^2\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$
$$+ \frac{\beta^2}{4}A_2^2\sin^2\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$
$$+ \frac{\alpha}{2}A_1A_2a_{n1}a_{n2}\cos\left(\frac{\pi t}{T_c}\right)\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$
$$+ \frac{\beta}{2}A_1A_2a_{n1}b_{n2}\cos\left(\frac{\pi t}{T_c}\right)\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$
$$+ \frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$

$$+\left[\frac{1}{2}A_1 a_{n1}\cos\left(\frac{\pi t}{T_c}\right)+\frac{\alpha}{2}A_2 a_{n2}\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right.$$

$$\left.+\frac{\beta}{2}A_2 b_{n2}\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right]n_c(t)+\frac{1}{4}n_c^2(t)$$

$$=\frac{1}{8}A_1^2+\frac{1}{8}A_2^2(\alpha^2+\beta^2)+\frac{1}{8}A_1^2\cos\left(\frac{2\pi t}{T_c}\right)$$

$$+\frac{1}{8}A_2^2(\alpha^2-\beta^2)\cos\left(\frac{2\pi(t-\Delta t)}{T_c}\right)$$

$$+\frac{\alpha}{4}A_1A_2a_{n1}a_{n2}\left[\cos\left(\frac{2\pi t}{T_c}-\frac{\pi\Delta t}{T_c}\right)+\cos\left(\frac{\pi\Delta t}{T_c}\right)\right]$$

$$+\frac{\beta}{4}A_1A_2a_{n1}b_{n2}\left[\sin\left(\frac{2\pi t}{T_c}-\frac{\pi\Delta t}{T_c}\right)-\sin\left(\frac{\pi\Delta t}{T_c}\right)\right]$$

$$+\frac{\alpha\beta}{4}A^2a_{n2}b_{n2}\sin\left(\frac{2\pi(t-\Delta t)}{T_c}\right)$$

$$+\left[\frac{1}{2}A_1 a_{n1}\cos\left(\frac{\pi t}{T_c}\right)+\frac{\alpha}{2}A_2 a_{n2}\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right.$$

$$\left.+\frac{\beta}{2}A_2 b_{n2}\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right]n_c(t)+\frac{1}{4}n_c^2(t) \qquad (204)$$

and

$$u_Q(t)=\frac{1}{4}A_1^2\sin^2\left(\frac{\pi t}{T_c}\right)+\frac{\alpha^2}{4}A_2^2\sin^2\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$

$$+\frac{\beta^2}{4}A_2^2\cos^2\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$

$$+\frac{\alpha}{2}A_1A_2b_{n1}b_{n2}\sin\left(\frac{\pi t}{T_c}\right)\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$

$$-\frac{\beta}{2}A_1A_2a_{n2}b_{n1}\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\sin\left(\frac{\pi t}{T_c}\right)$$

$$-\frac{\alpha\beta}{2}A_2^2a_{n2}b_{n2}\cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)$$

$$- \left[\frac{1}{2}A_1 b_{n1} \sin\left(\frac{\pi t}{T_c}\right) + \frac{\alpha}{2}A_2 b_{n2} \sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right.$$

$$\left. - \frac{\beta}{2}A_2 a_{n2} \cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right] n_s(t) + \frac{1}{4}n_s^2(t)$$

$$= \frac{1}{8}A_1^2 + \frac{1}{8}A_2^2(\alpha^2 + \beta^2) - \frac{1}{8}A_1^2 \cos\left(\frac{2\pi t}{T_c}\right)$$

$$+ \frac{1}{8}A_2^2(\beta^2 - \alpha^2) \cos\left(\frac{2\pi(t-\Delta t)}{T_c}\right)$$

$$+ \frac{\alpha}{4}A_1 A_2 b_{n1} b_{n2}\left[\cos\left(\frac{\pi\Delta t}{T_c}\right) - \cos\left(\frac{2\pi t}{T_c} - \frac{\pi\Delta t}{T_c}\right)\right]$$

$$- \frac{\beta}{4}A_1 A_2 a_{n2} b_{n1}\left[\sin\left(\frac{2\pi t}{T_c} - \frac{\pi\Delta t}{T_c}\right) - \sin\left(\frac{\pi\Delta t}{T_c}\right)\right]$$

$$- \frac{\alpha\beta}{4}A_2^2 a_{n2} b_{n2} \sin\left(\frac{2\pi(t-\Delta t)}{T_c}\right)$$

$$- \left[\frac{1}{2}A_1 b_{n1} \sin\left(\frac{\pi t}{T_c}\right) + \frac{\alpha}{2}A_2 b_{n2} \sin\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right.$$

$$\left. - \frac{\beta}{2}A_2 a_{n2} \cos\left(\frac{\pi(t-\Delta t)}{T_c}\right)\right] n_s(t) + \frac{1}{4}n_s^2(t) \qquad (205)$$

These results are then filtered by the audio low pass filter to give at the output for MSK

$$y_I(t) = \frac{\alpha}{4}A_1 A_2 a_{n1} a_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right)$$

$$- \left[\frac{\beta}{4}A_1 A_2 a_{n1} b_{n2} \sin\left(\frac{\pi\Delta t}{T_c}\right)\right]_{LP} + \left[\frac{1}{4}n_c^2(t)\right]_{LP} \qquad (206)$$

and

$$y_Q(t) = \frac{\alpha}{4}A_1 A_2 b_{n1} b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right)$$

$$+ \left[\frac{\beta}{4}A_1 A_2 a_{n2} b_{n1} \sin\left(\frac{\pi\Delta t}{T_c}\right)\right]_{LP} + \left[\frac{1}{4}n_s^2(t)\right]_{LP} \qquad (208)$$

For SFSK modulation, the analysis is much more complex. At the output of the square law device in the in-phase channel, the signal is (with $\Omega = t-\Delta t$):

$$
\begin{aligned}
u_I(t) = {} & \frac{1}{4}A_1^2 \cos^2\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right] \\
& + \frac{\alpha^2}{4}A_2^2 \cos^2\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& + \frac{\beta^2}{4}A_2^2 \sin^2\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& + \frac{\alpha}{2}A_1A_2a_{n1}a_{n2} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right] \\
& \cdot \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& + \frac{\beta}{2}A_1A_2a_{n1}b_{n2} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right] \\
& \cdot \sin\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& + \frac{\alpha\beta}{2}A_2^2a_{n1}b_{n1} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& \cdot \sin\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& + \left(\frac{1}{2}A_1a_{n1} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi t}{T_c}\right]\right. \\
& + \frac{\alpha}{2}A_2a_{n2} \cos\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right] \\
& \left. + \frac{\beta}{2}A_2b_{n2} \sin\left[\frac{\pi t}{T_c} - \frac{1}{4}\sin\frac{4\pi\Omega}{T_c} - \frac{\pi\Delta t}{T_c}\right]\right)n_c(t) \\
& + \frac{1}{4}n_c^2(t)
\end{aligned}
\tag{208}
$$

Expanding this gives (with $\omega_c = 2/T_c$)

$$u_I(t) = \frac{1}{8}A_1^2 + \frac{\alpha^2}{8}A_2^2 + \frac{\beta^2}{8}A_2^2 + \frac{1}{8}A_1^2 \cos\left[\omega_c t - \frac{1}{2}\sin(2\omega_c t)\right]$$

$$+ \frac{\alpha^2}{8}A_2^2 \cos\left[\omega_c t - \frac{1}{2}\sin(2\omega_c \Omega)\right]\cos(\omega_c \Delta t)$$

$$+ \frac{\alpha^2}{8}A_2^2 \sin\left[\omega_c t - \frac{1}{2}\sin(2\omega_c \Omega)\right]\sin(\omega_c \Delta t)$$

$$- \frac{\beta^2}{8}A_2^2 \cos\left[\omega_c t - \frac{1}{2}\sin(2\omega_c \Omega)\right]\cos(\omega_c \Delta t)$$

$$- \frac{\beta^2}{8}A_2^2 \sin\left[\omega_c t - \frac{1}{2}\sin(2\omega_c \Omega)\right]\sin(\omega_c \Delta t)$$

$$+ \frac{\alpha^2}{2}A_1 A_2 a_{n1} a_{n2} \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c t)\right]$$

$$\cdot \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right] \cos\left(\frac{\pi \Delta t}{T_c}\right)$$

$$+ \frac{\alpha^2}{2}A_1 A_2 a_{n1} a_{n2} \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c t)\right]$$

$$\cdot \sin\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right] \sin\left(\frac{\pi \Delta t}{T_c}\right)$$

$$+ \frac{\beta}{2}A_1 A_2 a_{n1} b_{n2} \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c t)\right]$$

$$\cdot \sin\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right]\cos\left(\frac{\pi \Delta t}{T_c}\right)$$

$$- \frac{\beta}{2}A_1 A_2 a_{n1} b_{n2} \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c t)\right]$$

$$\cdot \cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right] \sin\left(\frac{\pi \Delta t}{T_c}\right)$$

$$+ \frac{\alpha\beta}{2}A_2^2 a_{n1} b_{n2} \left[\cos\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right] \cos\left(\frac{\pi \Delta t}{T_c}\right)\right.$$

$$\left. + \sin\left[(\omega_c t/2) - \frac{1}{4}\sin(2\omega_c \Omega)\right] \sin\left(\frac{\pi \Delta t}{T_c}\right)\right]$$

$$\cdot \left[\sin\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\cos\left(\frac{\pi\Delta t}{T_c}\right)\right.$$

$$\left. - \cos\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\sin\left(\frac{\pi\Delta t}{T_c}\right)\right]$$

$$+ \left[\tfrac{1}{2}A_1 a_{n1}\cos\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c t)\right]\right.$$

$$+ \tfrac{\alpha}{2}A_2 a_{n2}\cos\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\cos\left(\frac{\pi\Delta t}{T_c}\right)$$

$$+ \tfrac{\alpha}{2}A_2 a_{n2}\sin\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\sin\left(\frac{\pi\Delta t}{T_c}\right)$$

$$+ \tfrac{\beta}{2}A_2 b_{n2}\sin\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\cos\left(\frac{\pi\Delta t}{T_c}\right)$$

$$\left. - \tfrac{\beta}{2}A_2 b_{n2}\cos\left[(\omega_c t/2) - \tfrac{1}{4}\sin(2\omega_c\Omega)\right]\sin\left(\frac{\pi\Delta t}{T_c}\right)\right] n_c(t)$$

$$+ \tfrac{1}{4}n_c^2(t) \qquad (209)$$

The sinusoids are now expressed as Bessel function expansions.

$$u_I(t) = \tfrac{1}{8}A_1^2 + \tfrac{\alpha^2}{8}A_2^2 + \tfrac{\beta^2}{8}A_2^2 + \tfrac{1}{8}A_1^2\sum_i J_i(1/2)\cos(1+2_i)\omega_c t$$

$$+ \tfrac{\alpha^2}{8}A_2^2\cos(\omega_c\Delta t)\sum_i J_i(1/2)\cos(\omega_c t + 2i\omega_c\Omega)$$

$$+ \tfrac{\alpha^2}{8}A_2^2\sin(\omega_c\Delta t)\sum_i J_i(1/2)\sin(\omega_c t + 2i\omega_c\Omega)$$

$$- \tfrac{\beta^2}{8}A_2^2\cos(\omega_c\Delta t)\sum_i J_i(1/2)\cos(\omega_c t + 2i\omega_c\Omega)$$

$$- \tfrac{\beta^2}{8}A_2^2\sin(\omega_c\Delta t)\sum_i J_i(1/2)\sin(\omega_c t + 2i\omega_c\Omega)$$

$$+ \tfrac{\alpha}{2}A_1 A_2 a_{n1} a_{n2}\cos\left(\frac{\pi\Delta t}{T_c}\right)\sum_i J_i(1/4)\cos\left(\frac{1+4i}{2}\omega_c t\right)$$

$$\cdot \sum_j J_j(1/4)\cos\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$+ \frac{\alpha}{2} A_1 A_2 a_{n1} a_{n2} \sin\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left(\frac{1+4i}{2}\omega_c t\right)$$

$$\cdot \sum_j J_j(1/4) \sin\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$+ \frac{\beta}{2} A_1 A_2 a_{n1} b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left(\frac{1+4i}{2}\omega_c t\right)$$

$$\cdot \sum_j J_j(1/4) \sin\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$- \frac{\beta}{2} A_1 A_2 a_{n1} b_{n2} \sin\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left(\frac{1+4i}{2}\omega_c t\right)$$

$$\cdot \sum_j J_j(1/4) \cos\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$+ \frac{\alpha\beta}{2} A_2^2 a_{n1} b_{n2} \cos^2\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$\cdot \sum_j J_j(1/4) \sin\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$- \frac{\alpha\beta}{2} A_2^2 a_{n1} b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) \sin\left(\frac{\pi\Delta t}{T_c}\right)$$

$$\cdot \sum_i J_i(1/4) \cos\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$\cdot \sum_j J_j(1/4) \cos\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$+ \frac{\alpha\beta}{2} A_2^2 a_{n1} b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) \sin\left(\frac{\pi\Delta t}{T_c}\right)$$

$$\cdot \sum_i J_i(1/4) \sin\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$\cdot \sum_j J_j(1/4) \sin\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$- \frac{\alpha\beta}{2} A_2^2 a_{n1} b_{n2} \sin^2\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \sin\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$\cdot \sum_j J_j(1/4) \cos\left[(\omega_c t/2) + 2j\omega_c\Omega\right]$$

$$+ \Bigg[\frac{1}{2} A_1 a_{n1} \sum_i J_i(1/4) \cos\left(\frac{1+4i}{2}\omega_c t\right)$$

$$+ \frac{\alpha}{2} A_2 a_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$+ \frac{\alpha}{2}A_2 a_{n2} \sin\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \sin\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$+ \frac{\beta}{2}A_2 b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \sin\left[(\omega_c t/2) + 2i\omega_c\Omega\right]$$

$$- \frac{\beta}{2}A_2 b_{n2} \sin\left(\frac{\pi\Delta t}{T_c}\right) \sum_i J_i(1/4) \cos\left[(\omega_c t/2) + 2i\omega_c\Omega\right] \Bigg] n_c(t)$$

$$+ \frac{1}{4}n_c^2(t) \qquad (210)$$

A careful examination of equation (210) shows that very few of these terms pass the output filter. The filtered output is:

$$y_I(t) = \frac{\alpha}{4}A_1 A_2 a_{n1} a_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) J_0^2(1/4)$$

$$- \left[\frac{\beta}{4}A_1 A_2 a_{n2} b_{n1} \sin\left(\frac{\pi\Delta t}{T_c}\right) J_0^2(1/4)\right]_{LP}$$

$$+ \left[\frac{1}{4}n_c^2(t)\right]_{LP} \qquad (211)$$

Through an identical analysis, the quadrature channel output is found to be:

$$y_Q(t) = \frac{\alpha}{4}A_1 A_2 b_{n1} b_{n2} \cos\left(\frac{\pi\Delta t}{T_c}\right) J_0^2(1/4)$$

$$+ \left[\frac{\beta}{4}A_1 A_2 a_{n2} b_{n1} \sin\left(\frac{\pi\Delta t}{T_c}\right) J_0^2(1/4)\right]_{LP}$$

$$+ \left[\frac{1}{4}n_s^2(t)\right]_{LP} \qquad (212)$$

Vita

Thomas J. Hall was born on September 4, 1949 in Ames, Iowa. He received a Bachelor of Science degree in Electrical Engineering from Iowa State University in 1973. Upon graduation and completion of Air Force ROTC, he was commissioned in the United States Air Force. After completing training at Keesler Technical Training Center in February 1974, he was assigned as a Communications-Electronics Engineer with the 1844th Electrical Engineering Squadron at Griffiss AFB in Rome, NY. In July 1977, he was assigned to TUSLOG Detachment 75, Pirinclik CDI in Diyarbakir, Turkey, where he served as Maintenance Supervisor until his assignment to the School of Engineering, Air Force Institute of Technology in June 1978.

Permanent address: 1601 Wilson Ave
Webster City, Iowa 50595

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER AFIT/GE/EE/79-15	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* INTERCEPT VULNERABILITY OF DIRECT SEQUENCE PSEUDO-NOISE ENCODED SPREAD SPECTRUM WAVEFORMS		5. TYPE OF REPORT & PERIOD COVERED MS Thesis 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Thomas J. Hall Capt USAF		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Air Force Institute of Technology (AFIT/EN) Wright-Patterson AFB, Ohio 45433		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Rome Air Development Center/DCI Griffiss AFB, NY 13441		12. REPORT DATE 15 December 1979 13. NUMBER OF PAGES 117
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)*		15. SECURITY CLASS. *(of this report)* Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

18. SUPPLEMENTARY NOTES

Approved for public release; IAW AFR 190-17

Joseph P. Hipps
Director of Public Affairs

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

INTERCEPT RECEIVER
SPREAD SPECTRUM
PSEUDO-NOISE CODING
PSEUDO-RANDOM CODING

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

Direct sequence pseudo-noise (PN) encoded spread spectrum (SS) waveforms are examined for their vulnerability to intercept and message reconstruction without knowledge of the PN code used. Two generic modulation formats are described and an intercept receiver model is proposed. Receiver outputs are calculated and it is shown that message reconstruction is possible for both generic modulation formats under appropriate conditions.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*